UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

"DISEÑO DE GUIAS DE LABORATORIO UTILIZANDO GNS3 PARA MEJORAR EL APROVECHAMIENTO DE RECURSOS DEL LABORATORIO OBTENIENDO UN MEJOR ESTUDIO DE NETWORKING"

TESIS

PARA OPTAR POR EL TÍTULO PROFESIONAL DE: INGENIERO ELECTRÓNICO

AUTORES:

Bach. JHONATAN JAVIER DÍAZ SUÁREZ
Bach. CARLOS ANTONIO PASCO HOYOS

LAMBAYEQUE - PERÚ
2014

UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

T E S I S

DISEÑO DE GUIAS DE LABORATORIO UTILIZANDO GNS3 PARA MEJORAR EL APROVECHAMIENTO DE RECURSOS DEL LABORATORIO OBTENIENDO UN MEJOR ESTUDIO DE NETWORKING.

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

AUTORES:

Bach. JHONATAN JAVIER DÍAZ SUÁREZ

Bach. CARLOS ANTONIO PASCO HOYOS

LAMBAYEQUE – PERÚ

2014

UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"

Facultad de Ciencias Físicas Y Matemáticas

Escuela Profesional de Ingeniería Electrónica

DISEÑO DE GUIAS DE LABORATORIO UTILIZANDO GNS3 PARA MEJORAR EL APROVECHAMIENTO DE RECURSOS DEL LABORATORIO OBTENIENDO UN MEJOR ESTUDIO DE NETWORKING.

Tesis Presentada por:

Bach. Jhonatan Javier Díaz Suárez

Bach. Carlos Antonio Pasco Hoyos

Jurado Calificador:

Ing. Victor Jara Sandoval

Presidente

Ing. Oscar Romero Cortéz

Secretario

Ing. Carlos Oblitas Vera

Vocal

Asesor:

Ing. Francisco Segura Altamirano

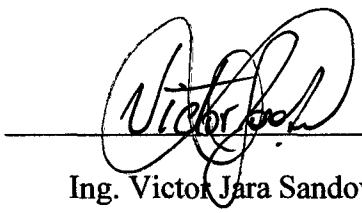
Tesis presentada por:

Bach. Díaz Suárez Jhonatan Javier

Bach. Pasco Hoyos Carlos Antonio

Como requisito para obtener el título de Ingeniero Electrónico.

Aceptada por la Facultad de Ciencias Físicas y Matemáticas y por la Escuela Profesional de Ingeniería Electrónica.

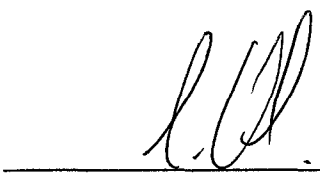


Ing. Victor Jara Sandoval

Presidente

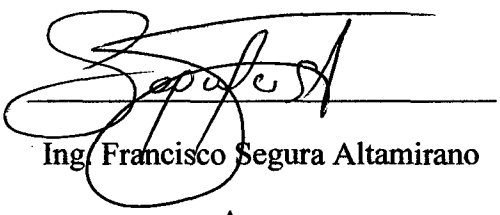
Ing. Oscar Romero Cortéz

Secretario



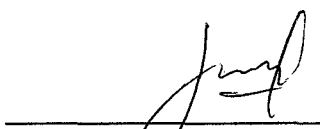
Ing. Carlos Oblitas Vera

Vocal



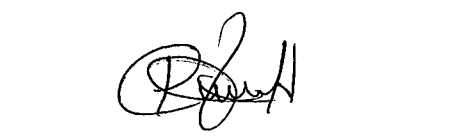
Ing. Francisco Segura Altamirano

Asesor



Bach. Jhonatan Díaz Suárez

Autor



Bach. Carlos Pasco Hoyos

Autor

LAMBAYEQUE NOVIEMBRE DEL 2014

DEDICATORIA:

A mis padres NELSON y MARIA, a mi hermano GINO, que siempre confiaron en mí, por su apoyo incondicional y que han sido el pilar importante para cumplir con esta meta.

JHONATAN DÍAZ SUÁREZ

A mis padres ENRIQUE y GINA, a mi hermano HUGO, y a mi esposa por ser ejemplo e inspiración que sostiene mis ideales y por hacer tener sentido a cada cosa que logro en esta vida.

CARLOS PASCO HOYOS

ÍNDICE GENERAL

CAPÍTULO IV: DISEÑO DE GUÍAS DE LABORATORIO CON SIMULADOR GNS3.

CAPÍTULO V: DISEÑO DE DESAFÍOS DE LABORATORIO CON SIMULADOR GNS3 Y EQUIPOS FÍSICOS.

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Mediante la aplicación de la teoría y conceptos básicos de networking, se realiza un conjunto de 17 guías de laboratorio y 17 desafíos de laboratorio, los mismos permitirán al Ingeniero instructor contrastar diferentes conceptos de redes junto a los estudiantes de la Escuela Profesional de Ingeniaría Electrónica. Como herramienta de simulación se utiliza GNS3 el cual es programa gratuito que nos permite procesar simulaciones graficas de redes complejas, el cual también puede ser interconectado con equipos reales, puede ser utilizado en múltiples sistemas operativos, incluyendo Windows y Linux. Las guías y desafíos de laboratorio permiten al estudiante ir paso a paso configurando y entendiendo los diferentes protocolos de enrutamiento que rigen las comunicaciones.

CAPITULO I

PLANTEAMIENTO METODOLOGICO

1.1 PLANTEAMIENTO DEL PROBLEMA CIENTÍFICO

Actualmente la escuela de Ingeniería Electrónica cuenta con equipos de Networking de gama media, que supera inclusive los de muchas academias Cisco, pero los instructores a cargo de las asignaturas no cuentan con la capacitación adecuada, además que la cantidad de equipos es insuficiente para la gran cantidad de estudiantes, haciéndose difícil que todos tengan acceso a estos equipos, los equipos son de muy alto costo, por lo cual se hace difícil que se pueda implementar el laboratorio con equipos de última generación en un periodo de tiempo corto, por tal motivo se ha buscado otras alternativas como es un emulador de redes.

Además que las practicas se desarrollan siguiendo las guías de los cursos de CCNA, pero como mencionamos antes el Laboratorio de Electrónica cuenta con equipos de otras series a las usadas por las mismas, por lo que se hace necesario unas guías de laboratorio que hagan uso de todas las posibilidades ofrecidas por estos equipos, además que gracias a los emuladores podemos realizar diseños de redes medianas que se interconecten a los equipos físicos, aumentando el abanico de situaciones con las que el estudiante se puede encontrar en su desarrollo profesional.

La emulación de equipos constituye un papel muy importante como una herramienta para capacitación de los estudiantes en circunstancias en las que la práctica real puede ser muy costosa, peligrosa o ambas.

1.2 ANTECEDENTES

En el año **2011** en la Universidad Politécnica de Cataluña fue presentado el proyecto de tesis cuyo autor fue Lisset Díaz Cervantes, donde se realizó una evaluación de la herramienta GNS3 que consistía en la conectividad con enrutadores físicos y analizar el rendimiento entre el equipo real y virtual.

Para medir el rendimiento de los dispositivos realizo 3 pruebas: la primera tuvo como objetivo cuantificar el tiempo de respuesta de los equipos, la segunda trato de medir la velocidad máxima de transmisión de datos alcanzada en el enlace sin que se produzcan pérdidas de paquetes, y la última prueba se centró en mostrar el Jitter de un enlace; para las dos últimas pruebas utilizó un programa llamado "Iperf".

Después de la realización de las pruebas se llegó a las siguientes conclusiones:

- Es posible la interconexión de emuladores que trabajan conjuntamente.
- La conexión externa es transparente a los equipos.
- Los routers virtuales soportan ser configurados como agentes SNMP para enviar sus datos al servidor MRTG.

En el **2012** en la Universidad Tecnológica de Ecuador, se estudió, Diseñó y Simuló en GNS3 unas guías de laboratorio para Redes de Datos y Networking de la Facultad de Electrónica de la Universidad Israel.

Consistió en la creación de guías de laboratorio de conceptos básicos de redes, las mismas permitían al Ingeniero instructor contrastar diferentes conceptos de redes junto a los estudiantes. Las guías de laboratorio permitieron al estudiante ir paso a paso configurando y entendiendo los diferentes protocolos que rigen las comunicaciones.

Obteniendo así un emulador muy útil ya que consiste en ejecutar efectivamente un IOS como si fuera un enrutador, es decir, se puede acceder a todas las características del IOS y la plataforma tal como si fuera un enrutador real.

1.3 FORMULACIÓN DEL PROBLEMA CIENTÍFICO

¿Cómo podemos diseñar las guías de laboratorio, para mejorar el aprovechamiento y suplir la usencia de equipos de laboratorio de la Escuela Profesional de Ingeniería Electrónica de la FACFyM/UNPRG y adquirir mejores habilidades y competencias en el campo de Networking, logrando así un buen nivel competitivo en la región, el país y el mundo?

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL:

- Diseñar guías de prácticas de laboratorio para el uso del simulador GNS3 para las asignaturas de Teleinformática I y II.

1.4.2 OBJETIVOS ESPECIFICOS:

a) Estudiar la transmisión de datos (tráfico, protocolos, tablas de enrutamiento, etc.) existente entre routers emulados usando GNS3 y routers reales.

b) Mostrar la posibilidad de funcionamiento conjunto de varios emuladores GNS3 y redes reales ampliando así "tamaño" del laboratorio de Electrónica.

c) Analizar el rendimiento de redes formadas por enrutadores emulados usando GNS3 y redes mixtas que también contienen routers reales.

d) Proporcionar a los estudiantes de electrónica una alternativa económica para adquirir las habilidades y competencias en el campo del networking.

1.5. JUSTIFICACIÓN E IMPORTANCIA

Porque elaborando las guías de laboratorio se podrá sustituir la ausencia de equipos físicos, ya que no se puede llevar acabo un control adecuado del aprendizaje de los mismos, pues debido a esta falta de equipos los trabajos son grupales lo que no asegura que todos los estudiantes adquieran las habilidades técnicas requeridas en esta área.

Por consecuencia se obtendrá un área de trabajo más amplio, y poder realizar diversos estudios y análisis de los conocimientos de networking, con la ayuda de los emuladores de redes ya que en ellos se puede ejecutar cualquier tipo de configuración sea simple o compleja como si se estuviese trabajando directamente con un equipo real. Como herramienta de simulación se utilizará GNS3 el cual es un software gratuito que puede ser utilizado en múltiples sistemas operativos, es un entorno grafico de simulación de redes complejas utilizando dispositivos emulados CISCO como routers, switches, etc.

Con este software es posible probar y experimentar nuevas funcionalidades sin correr el riesgo de poner en peligro la integridad de una red real con configuraciones erróneas, el emulador GNS3 presenta capacidades que merecen ser estudiadas y analizadas profundamente para

conocer cuál es el rendimiento de los dispositivos que emula y cuál es el comportamiento cuando se forman redes con dispositivos emulados o con dispositivos reales.

Cuando se trabaja con redes es de suma importancia conocer la manera en cómo se están comunicando los datos, para de esta manera realizar un análisis que permita determinar la calidad del enlace de comunicaciones, para ello tenemos que tomar en cuenta los parámetros más comunes para chequear el comportamiento de una red, siendo los primordiales la eficiencia, el throughput y el retraso o latencia, los cuales sufren los paquetes debido a las congestiones que pueden encontrar entre el origen y el destino de la red.

1.6 FORMULACIÓN DE LA HIPOTESIS

Si implementamos guías de laboratorio de networking usando el simulador de redes GNS3 y los equipos físicos del Laboratorio, las cuales constaran de una estructura organizada de acuerdo a la temática que se basan las asignaturas de Teleinformática I y Teleinformática II, asimismo el diseño de las guías de laboratorio consiste en:

- Revisión teórica de la práctica a realizar
- Objetivos a tratar en la práctica de laboratorio.
- Escenario de Laboratorio.
- Diagrama de la topología.
- Realizar las configuraciones necesarias para la práctica.
- Verificar y probar las configuraciones realizadas.
- Analizar el tráfico de paquetes.
- Contestar preguntas necesarias para la realización de las prácticas.
- Entregar informes de lo realizado en clases.
- Sacar conclusiones y recomendaciones de lo elaborado en las prácticas.

Por ende las guías de laboratorio permitirán a los estudiantes de Ingeniería Electrónica de la Facfym/UNPRG, profundizar los conceptos teóricos y prácticos de Networking, poniéndolos a un buen nivel competitivo.

CAPITULO II

MARCO TEORICO REFERENCIAL

2.1. Fundamentos de Networking

2.1.1 Enrutamiento

El *encaminamiento* (a veces *conocido* por el anglicismo ruteo o enrutamiento) es el mecanismo con el que se hacen llegar paquetes desde su origen a su destino final, siguiendo un camino o ruta a través de la red. En una red grande o en un conjunto de redes interconectadas el camino a seguir hasta llegar al destino final puede suponer transitar por muchos nodos intermedios.

Asociado al encaminamiento existe el concepto de métrica, que es una medida de lo "bueno" que es usar un camino determinado. La métrica puede estar asociada a distintas magnitudes: distancia, coste, retardo de transmisión, número de saltos, etc., o incluso a una combinación de varias magnitudes. Si la métrica es el retardo, es mejor un camino cuyo retardo total sea menor que el de otro. Lo ideal en una red es conseguir el encaminamiento óptimo: tener caminos de distancia (o coste, o retardo, o la magnitud que sea, según la métrica) mínimos. Típicamente el *encaminamiento es una función implantada en la capa 3 (capa de red) del modelo* de referencia OSI.[1]

2.1.2 Direccionamiento de la Red

Una red es un conjunto de dispositivos que comparten recursos, cada dispositivo en la red debe estar definido con una dirección IP para que pueda comunicarse. Una dirección IP se representa en formato binario siendo un conjunto de 32 bits, a su vez se divide en 4 grupos de 8 bits conocidos como octetos, pero para facilidad del usuario final las direcciones IP se expresan en formato decimal de esta manera se tiene por ejemplo la dirección de host 192.168.1.1.[2]

Cierta cantidad de bits representa la porción de red mientras que otro conjunto de bits la porción de host; quien realiza esta separación es la máscara de red. Los dispositivos que se encuentren en la misma red pueden comunicarse sin la necesidad de poner un Gateway o puerta de enlace. El Gateway es un dispositivo que conoce como llegar a redes remotas.

Actualmente se manejan subredes con máscara de longitud variable VLSM, se puede asignar a una red el número de host adecuado sin que se desperdicie el direccionamiento. Utilizar VLSM es una buena práctica y es útil especialmente en

[1] Tomado de: http://upcommons.upc.edu/pfc/bitstream/2099.1/11730/1/PFC.pdf
[2] Tomado de: http://los9mm.over-blog.es/article-29399073.html

el diseño de una red, como consideración se tiene que pensar en la escalabilidad siempre que se encuentre en esta fase de diseño.

2.1.3 Mascara de Subred

La máscara de subred al igual que una dirección IP es un conjunto de dígitos binarios de 32 bits que se encuentran separados en octetos de 8 bits, a cada octeto se le separa con un punto por lo que se tiene 4 octetos; la función principal de la máscara es determinar cuál es la porción de red y de host de una dirección IP.

"Por ejemplo, una máscara de 20 bits se escribiría 255.255.240.0, es decir una dirección IP con 20 bits en 1 seguidos por 12 bits en 0, pero separada en bloques de a 8 bits escritos en decimal. La máscara determina todos los parámetros de una *subred: dirección de red, dirección de difusión (broadcast)* y *direcciones* asignables a nodos de red (hosts)".[3]

2.1.4 VLSM y CIDR

Anteriormente se manejaban redes con clase es decir siempre una dirección IP pertenecía a la clase A, B o C y la máscara de estas clases era fija: /8, /16, /24 respectivamente. El problema de las redes con clase era que se desperdiciaba direcciones IP y si por ejemplo se necesitaba 10 direcciones se debía utilizar una red clase C que tiene un total de 254 direcciones disponibles. VLSM es el resultado del proceso por el cual se divide una red o subred en subredes más pequeñas cuyas máscaras son diferentes según se adaptan a las necesidades de hosts por subred.

"La máscara de subred de tamaño variable (variable length subnet mask, VLSM) representan otra de las tantas soluciones que se implementaron para el agotamiento de direcciones IP (1987) y otras como la división en subredes (1985), el enrutamiento de interdominio CIDR (1993), NAT y las direcciones ips privadas. Otra de las funciones de VLSM es descentralizar las redes y de esta forma conseguir redes más seguras y jerárquicas".[4]

CIDR significa Class Inter Domain Routing es el sinónimo de sumarización de rutas o creación de superredes. Una vez que una trama llega al Router se examina la tabla de enrutamiento, en donde se observa la mejor ruta para llevar el paquete al destino; el proceso de búsqueda en la tabla de enrutamiento consume recursos del equipo razón por la que mientras más eficiente es la búsqueda se tiene menor latencia. Una súper red consiste en reunir varias redes contiguas, que se encontraban de manera independiente en la tabla de enrutamiento y escribirla como una sola ruta.

---

[3] Tomado de: http://es.wikipedia.org/wiki/Subred

[4] Tomado de: http://mikrotikxperts.com/index.php/2013-03-28-19-49-36/conocimientos-basicos/160-tutorial-vlsm-cidr

2.1.5 Dynamic Host Configuration Protocol (DHCP)

DHCP significa protocolo de configuración dinámica de host y permite que un dispositivo conectado a la red pueda obtener de manera dinámica los parámetros de red como la dirección IP, la Máscara de subred, el Gateway y el DNS. En el servicio de DHCP se tiene un modelo cliente/servidor, como se observa en el gráfico el cliente realiza una solicitud de broadcast (a todos los dispositivos de la red), en donde el servidor responde a la solicitud del cliente con los parámetros de red necesarios.

La ventaja del servicio de DHCP es que se tiene un control del direccionamiento asignado, en una red, una dirección IP no puede repetirse ya que causaría inconvenientes y no se podría utilizar los recursos de la red por parte de las máquinas involucradas.

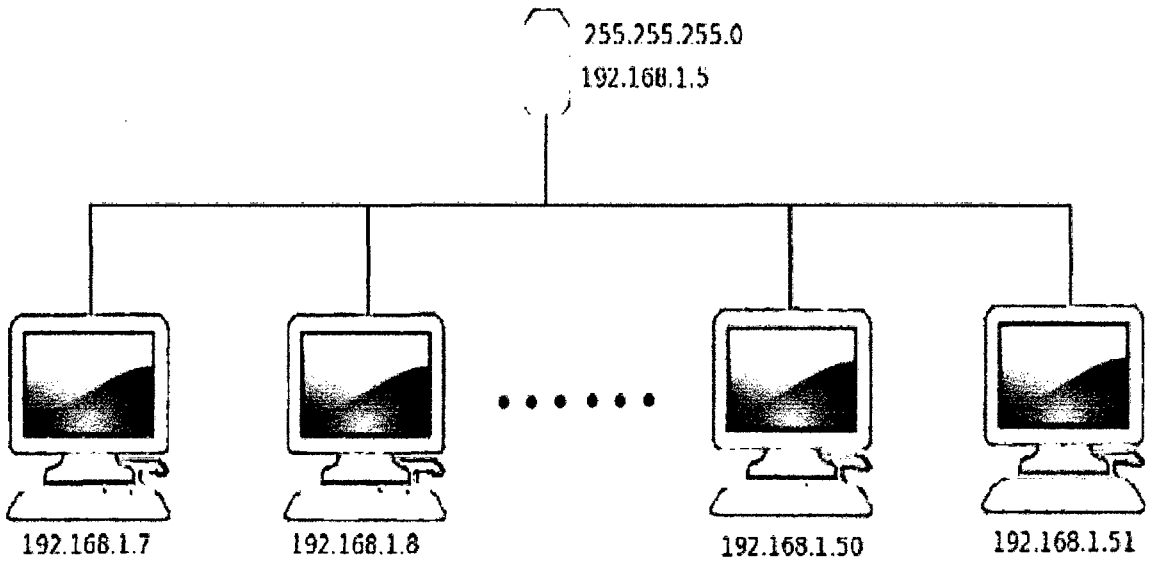


Fig. 2.1 Funcionamiento de DHCP[5]

2.1.6 QoS (Calidad de servicio)

En un inicio el tráfico que se tenía en una red era únicamente datos jamás se pensó que por dicha red va a atravesar tráfico en tiempo real como voz o video. La calidad de Servicio es un parche que se utilizó para la red de datos debido a que el tráfico en tiempo real tiene ciertos requerimientos para que funcione adecuadamente. En el siguiente gráfico se puede observar que no todo el tráfico es igual y que cada aplicación tiene requerimientos especiales:

[5] Tomado de: http://www.see-my-ip.com/tutoriales/protocolos/dhcp.php

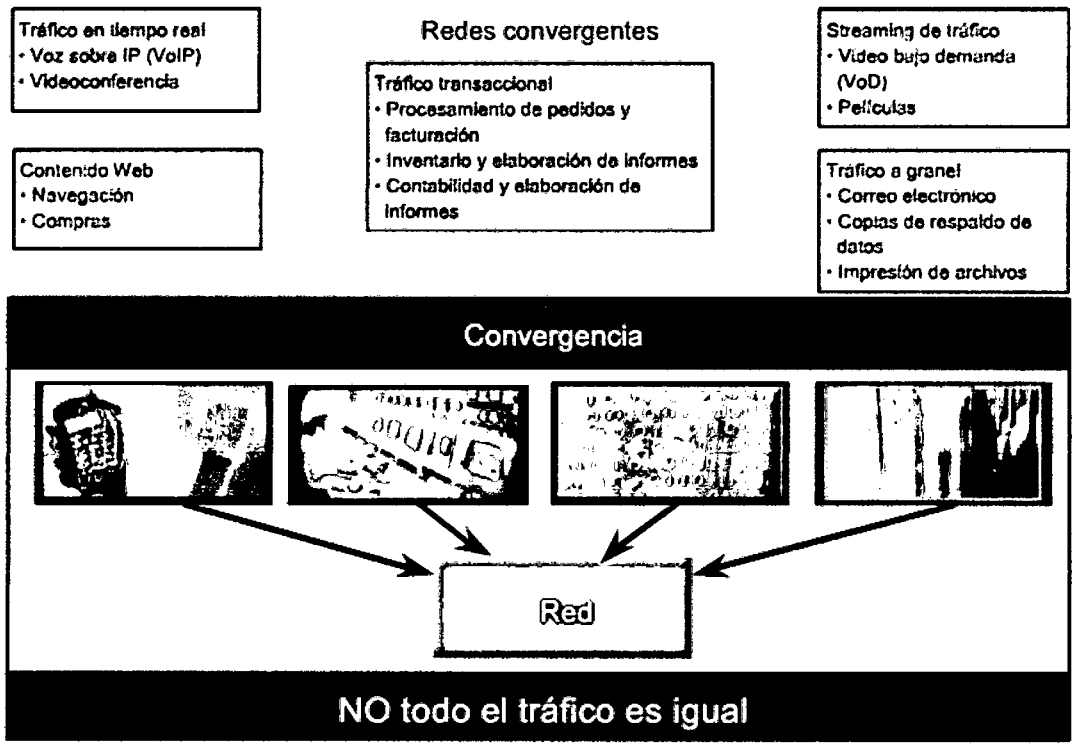
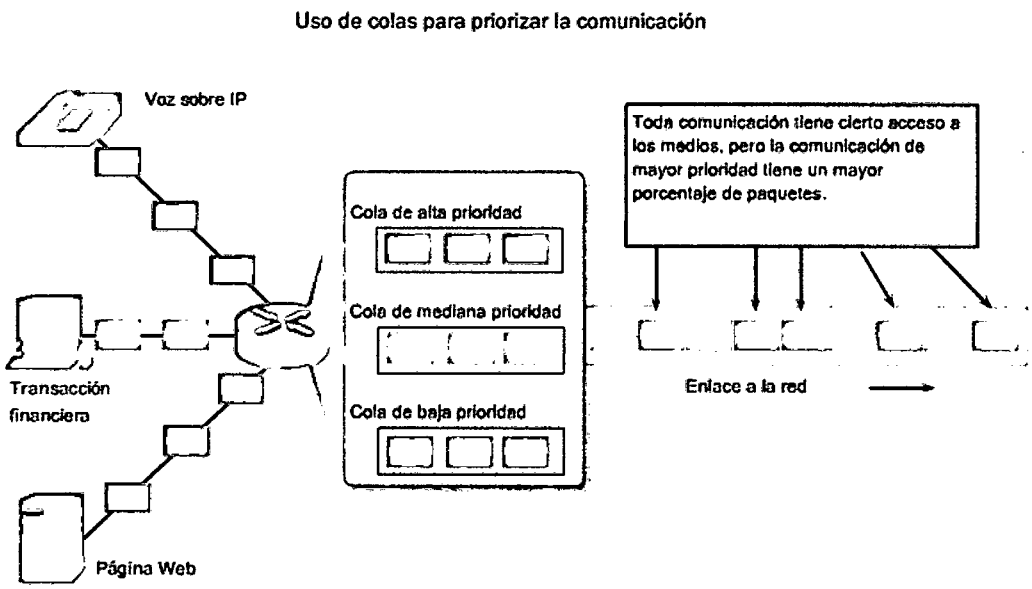


Fig. 2.2 Redes convergentes[6]

Para configurar calidad de servicio se clasifica a cada aplicación, con el fin de dar un trato especial o garantizar ancho de banda para su correcto funcionamiento. Para dar prioridad al tráfico se utiliza el concepto de colas. A continuación se presenta un gráfico en donde se puede observar los distintos tipos de tráfico que puede atravesar la red:



[6] Tomado de: Cisco CCNA 1

Fig. 2.3 Priorización de tráfico en QoS[7]

La configuración de calidad de servicio se debe realizar en todos los equipos intermedios como routers o switches, y se deben respetar las marcaciones realizadas. Los paquetes deben marcarse lo más cercano al origen como sea posible.

2.2 Protocolos de Enrutamiento para Redes LAN

El enrutamiento es fundamental para cualquier red de datos, ya que transfiere información a través de una internetwork de origen a destino.

Debido a la evolución de las redes y a su complejidad cada vez mayor, han surgido nuevos protocolos de enrutamiento. La figura muestra la clasificación de los protocolos de enrutamiento:

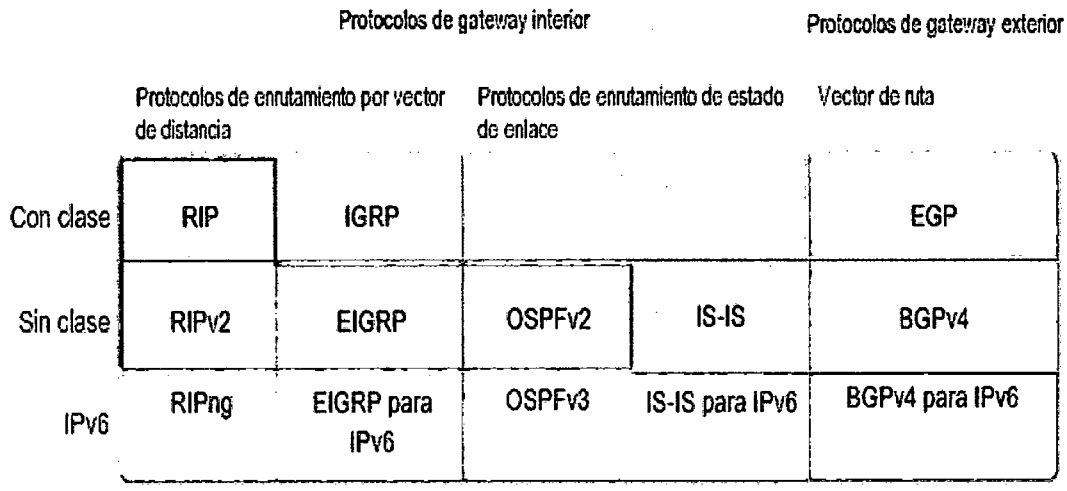


Fig. 2.4 Protocolos de enrutamiento[8]

2.2.1 Enrutamiento Estático

Un Router tiene redes directamente conectadas y redes remotas. Las redes directamente conectadas son las que se configuran en las interfaces del Router, y las redes remotas son aquellas que se encuentran en otro Router y que hay que tener una ruta en la tabla de enrutamiento para poder alcanzarlas. Para llegar a las redes remotas se tienen dos opciones que son configurar enrutamiento estático y dinámico. En el enrutamiento estático hay que configurar rutas en cada router de manera manual, se debe tomar en cuenta que un principio de enrutamiento es tener rutas de ida y de retorno para una ruta. Las rutas estáticas no requieren tanto

[7] Tomado de: Cisco CCNA 1
[8] Tomado de: Cisco CCNA 2

procesamiento como el enrutamiento dinámico. Para configurar una ruta estática se tiene dos opciones:

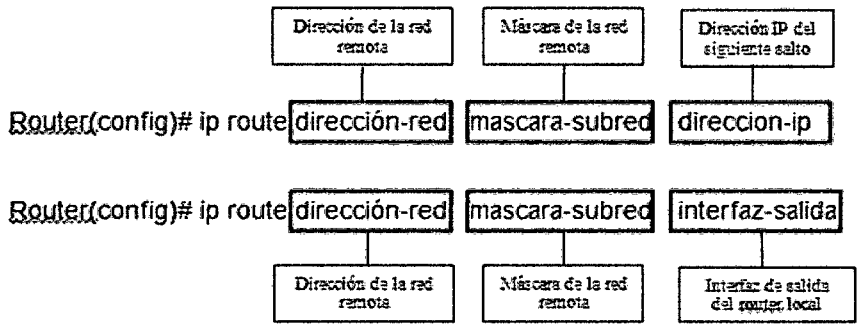


Fig. 2.5 Rutas Estáticas[9]

2.2.2 Rip versión 1 y 2

RIP es un protocolo de enrutamiento dinámico IGP (interior Gateway protocol), es decir un protocolo que se puede utilizar dentro de una empresa y que permite realizar el intercambio de rutas en forma dinámica. En la actualidad existen tres versiones diferentes de RIP, las cuales son:

RIPv1:

- No soporta subredes CIDR (superredes)
- No soporta autentificación de los mensajes de enrutamiento.
- No se usa actualmente.
- Protocolo de enrutamiento con clase (no envía la máscara de subred en las actualizaciones de enrutamiento).

RIPv2:

- Soporta subredes
- Soporta CIDR y VLSM.
- Soporta autenticación de mensajes

Ventajas e Inconvenientes Ventajas de RIP

- Es un protocolo estándar
- Fácil de configurar respecto a otros protocolos.

Desventajas de RIP

- No es muy escalable su métrica son los saltos y el tope máximo es 15 routers.

[9] Tomado de: Tesis de María Fernanda Tamayo Domínguez

2.2.3 EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP es un protocolo de enrutamiento dinámico IGP (interior Gateway protocol), es un protocolo híbrido debido a que usa características de los algoritmos de vector distancia y estado de enlace. IGRP es su predecesor siendo los dos propietarios de Cisco. Para la métrica utiliza algunos parámetros como el ancho de banda, retardo, confiabilidad y carga, el algoritmo que utiliza es el Dual para calcular las mejores rutas, agregarlas a la tabla de enrutamiento y realizar la convergencia rápidamente. EIGRP puede enrutar diferentes protocolos de capa 3 como IP, IPX y Apple Talk. La principal diferencia con RIP es que no usa únicamente la tabla de enrutamiento sino que maneja otra tabla conocida como tabla de topología en donde se almacenan las rutas de backup en el caso de que la ruta principal falle, de esta manera se tiene un mejor tiempo de convergencia. La convergencia consiste en que todos los routers tengan la información completa del estado de la red. Además se tiene una tercera tabla conocida como tabla de vecinos donde se encuentran los routers que también tienen configurado el protocolo EIGRP.

Otra diferencia importante con respecto a RIP es que no envía toda la tabla de enrutamiento cada cierto tiempo sino que envía actualizaciones parciales es decir solo los cambios que se han producido y a los routers que lo necesitan. A continuación se puede observar un gráfico con la distancia administrativa de EIGRP y otros protocolos de enrutamiento dinámico:

Distancias administrativas predeterminadas

Origen de la ruta	Distancia administrativa
Conectado	0
Estático	1
Ruta sumarizada de EIGRP	5
BGP externo	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	170
BGP interno	200

Fig. 2.6 Distancias Administrativas predeterminadas[10]

[10] Tomado de Cisco CCNA 2

La distancia administrativa es un valor asignado a cada protocolo de enrutamiento dinámico, red directamente conectada o ruta estática para ver quien tiene mayor preferencia en el caso de encontrarse configurado en el mismo equipo. Al igual que rip v2 y OSPF, EIGRP permite manejar autenticación al enviar las actualizaciones de enrutamiento.

EIGRP es un protocolo muy bueno pero tiene la desventaja de ser propietario, por lo cual no puede ser utilizado con equipos de otras marcas que no sean Cisco.

2.2.4 OSPF (Open Shortest Path First)

"Open Shortest Path First es un protocolo de Gateway interior (IGP), utiliza el algoritmo de Dijkstra que le permite calcular las mejores rutas hacia el destino, es protocolo de estado que usa el costo como métrica. El costo se refiere al ancho de banda, envía los paquetes hacia el destino por donde existe mayor ancho de banda. Una de las principales características por ser un vector de estado de enlace es que cada router tiene conocimiento completo de la topología de la red para lo cual tiene una base de datos del estado de los enlaces de todos los routers que hablan OSPF. OSPF es un protocolo muy utilizado en redes grandes como proveedores de servicio, en el Ecuador la mayoría de proveedores de servicio (ISP) tienen configurado en su backbone OSPF como protocolo de enrutamiento dinámico. Acepta VLSM y CIDR, actualmente se maneja IPV6 con la versión 3 de OSPF; una ventaja indiscutible de OSPF es que es muy escalable, maneja el concepto de áreas para grandes redes.

Para evitar el consumo de ancho de banda se maneja el concepto de DR y BDR, el DR o router designado recibe las actualizaciones de los routers dentro de su área y es el encargado de distribuir esa información al resto de los routers, el BDR o router designado de backup es un equipo que se encuentra listo en el caso que el DR falle.

2.2.5 BGP

Border Gateway Protocol (BGP) es un protocolo de enrutamiento por vector de distancia usado comúnmente para enrutar paquetes entre dominios, estándar en Internet. BGP gestiona el enrutamiento entre dos o más routers que sirven como routers fronterizos para determinados Sistemas Autónomos. BGP versión 4 (BGP-4), es el protocolo de enrutamiento entre dominios elegido en Internet, en parte porque administra eficientemente la agregación y la propagación de rutas entre dominios. Aunque BGP-4 es un protocolo de enrutamiento exterior, también puede utilizarse dentro de un SA como un conducto para intercambiar actualizaciones BGP. Las conexiones BGP dentro de un SA son denominadas BGP interno (IBGP), mientras que las conexiones BGP entre routers fronterizos (distintos SA) son denominadas BGP externo (EBGP). BGP-1, 2 y 3 están obsoletos. Para la configuración de OSPF se requiere un número de Sistema

Autónomo, ya que se pueden ejecutar distintos procesos OSPF en el mismo routers. BGP se especifica en las RFC 1163, 1267 y 1771, que definen las versiones 2, 3 y 4 de BGP, respectivamente.[11]

Los iguales BGP se dividen en dos categorías: Los iguales BGP de distintos sistemas autónomos que intercambian información de enrutamiento son iguales BGP externos (EBGP). Los iguales BGP del mismo sistema autónomo que intercambian información de enrutamiento son iguales BGP internos (IBGP).

La selección de ruta óptima BGP se basa en la longitud de la ruta de acceso del sistema autónomo para una ruta de red. La longitud se define como el número de sistemas autónomos distintos necesarios para acceder a la red. Cuanto menor sea la distancia, más apetecible será la ruta de acceso. A través del uso de controles administrativos, BGP es uno de los protocolos de enrutamiento más flexibles y totalmente configurables disponibles.

Un uso típico de BGP, para una red conectada a Internet a través de varios ISP, es el uso de EBGP con los ISP, así como el uso de IBGP en la red interna, para así ofrecer una óptima selección de rutas. Las redes conocidas de otros sistemas autónomos a través de EBGP se intercambiarán entre los iguales IBGP. Si sólo hubiera un ISP, valdría con utilizar una ruta resumen o predeterminada para la salida a internet.

Tenga en cuenta que los routers BGP publican las rutas conocidas de un igual BGP a todos sus otros iguales BGP. Por ejemplo, las rutas conocidas a través de EBGP con un ISP se volverán a publicar a los iguales IBGP, que a su vez volverán a publicarlos a otros ISP a través de EBGP. Mediante la publicación reiterada de rutas, la red puede pasar a ser una red de tránsito entre los proveedores con los que se conecte. BGP puede parametrizarse tanto para que la red interna actúe como una red de tránsito, como para que no.

2.3 Protocolos de Enrutamiento para Redes WAN

Una WAN es una red de comunicación de datos que opera más allá del alcance geográfico de una LAN. Las WAN se diferencian de las LAN en varios aspectos. Mientras que una LAN conecta computadoras, dispositivos periféricos y otros dispositivos de un solo edificio u de otra área geográfica pequeña, una WAN permite la transmisión de datos a través de distancias geográficas mayores.

A continuación se muestra en la gráfica un resumen de las diferentes opciones que se dispone a nivel WAN.

[11] Tomado de: http://www.guillesql.es/Articulos/Manual_Cisco_CCNA_Protocolos_Enrutamiento.aspx

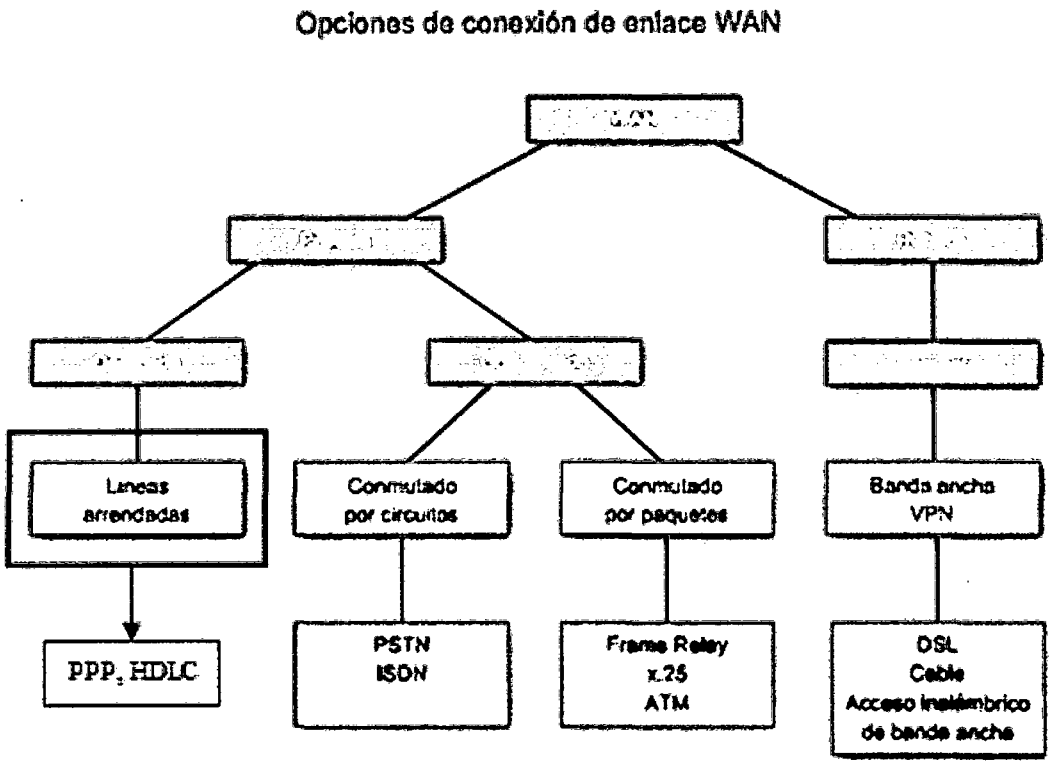


Fig. 2.7 Opciones de conexión de enlaces WAN[12]

Una red WAN se utiliza cuando se tiene áreas geográficas extensas y principalmente cuando se paga a un proveedor por el servicio

2.3.1 PPP (Point-to-Point Protocol)

El protocolo Punto Punto permite realizar conexiones WAN, es un protocolo de capa 2 que se utiliza generalmente en conexiones seriales también conocidas como líneas arrendadas. Una línea arrendada lleva su nombre porque se debe pagar a un proveedor por el servicio debido a que la empresa no tiene infraestructura propia para proporcionar conectividad. Para realizar una conexión punto a punto se puede utilizar cualquier tipo de medios ya sean guiados como cobre o fibra óptica o no guiados es decir utilizando medios inalámbricos. En el siguiente gráfico se puede observar que PPP junto a HDLC son protocolos de enlace de datos punto a punto dedicados

[12] Tomado de: Cisco CCNA 4

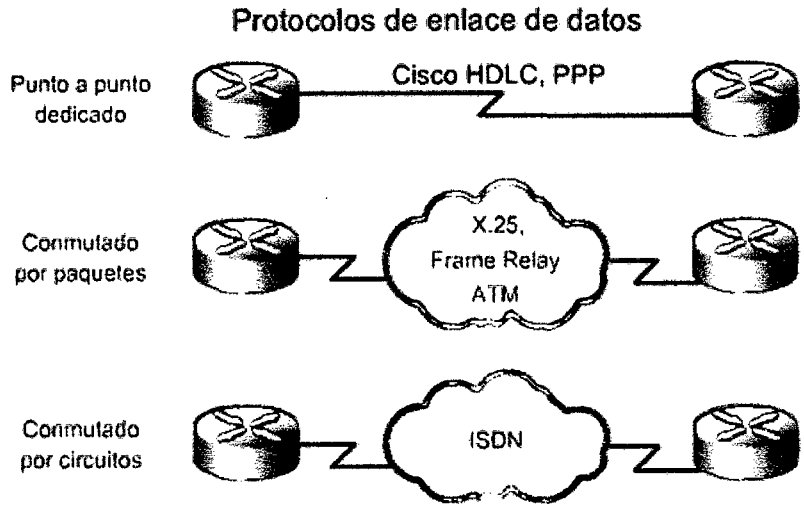


Fig. 2.8 Protocolos de enlaces de Datos[13]

Al momento de que un paquete atraviese la WAN debe encapsularse en una trama PPP y además permite brindar seguridad con los protocolos para autenticación PAP o CHAP.

2.3.2 Frame Relay

Es un protocolo de capa 2 que utiliza la tecnología de conmutación por paquetes, es similar a X25 pero más sencillo, no realiza control de flujo ni control de errores, esa es la razón por que se tiene menor latencia (tiempo de un paquete en viajar desde el origen hasta el destino).

Como se puede observar en el gráfico maneja circuitos virtuales (conexión entre dos DTE) los mismos que se identifican mediante un DLCI que es un número cualquiera asignado por el proveedor, con la particularidad que dicho número tiene únicamente significado local es decir solo en el segmento, y se puede tener varios circuitos virtuales en un canal físico.

[13] Tomado de: Cisco CCNA 4

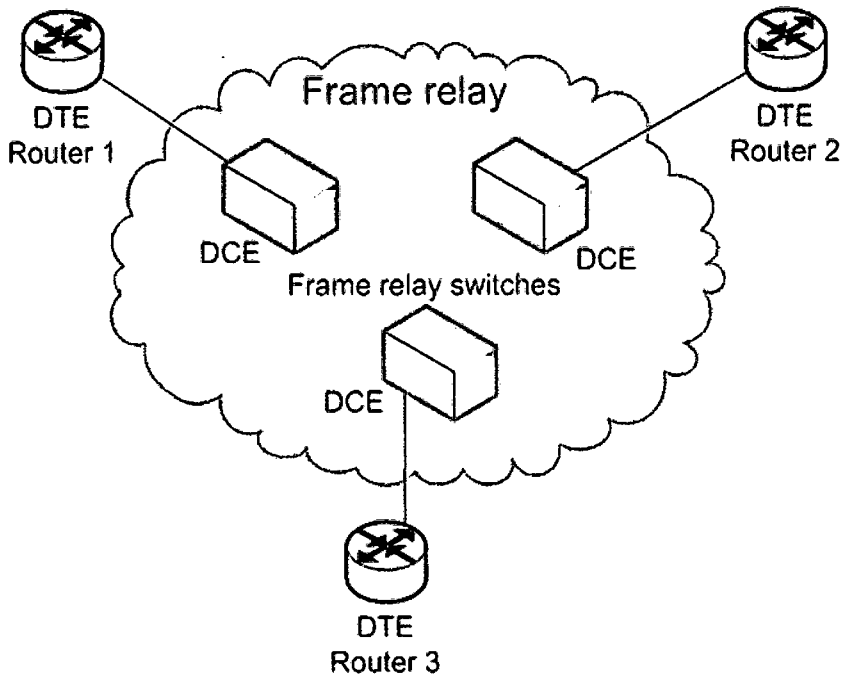


Fig. 2.9 Frame Relay[14]

La red del proveedor que ofrece Frame Relay está constituida por un conjunto de Switch unidos a través de troncales que permite realizar la conmutación de paquetes. Frame Relay se convirtió en la tecnología más utilizada del mundo por el precio, actualmente desplazada por MPLS.

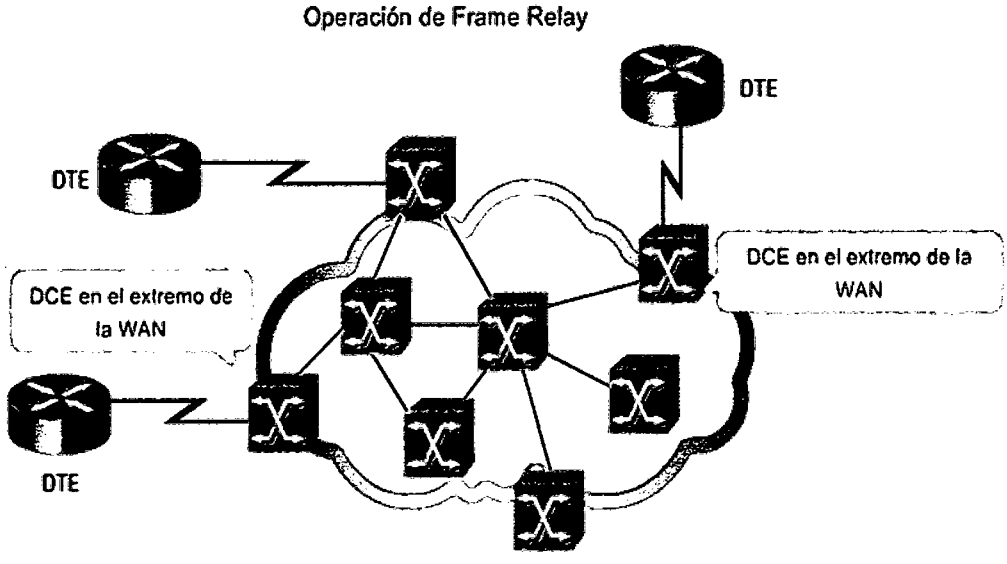


Fig. 2.10 Operación de Frame Relay[15]

Existe dos tipos de circuitos virtuales, los circuitos virtuales conmutados que se establecen de manera automática liberando recursos una vez que se deja de transmitir datos y los circuitos virtuales permanentes como su nombre lo indica

[14] Tomado de: http://en.wikipedia.org/wiki/File:Frame_relay.jpg
[15] Tomado de: Cisco CCNA 4

así se termine de transmitir datos el circuito permanece establecido. El dispositivo de acceso a la red Frame Relay se denomina FRAD tiene varias conexiones a diferentes puntos y como se mencionó anteriormente cada uno de los circuitos virtuales se identifican a través del DLCI. Frame Relay maneja topologías de estrella en donde se tiene un sitio central y varias sucursales, malla parcial y malla completa para ofrecer redundancia, es una tecnología muy versátil.

2.3.3 MPLS

Multiprotocol Label Switching (MPLS) es un mecanismo de transporte de datos estándar, emergente del IETF (RFC 3031). Opera entre la capa de enlace de datos y la capa de red del modelo OSI, se encontraría en la capa 2.5, entre la capa 2 y 3. El hecho de que se encuentre entre dos capas, le proporciona el nombre de "Multi Protocol". Este hecho le da la ventaja de poder usar las características de los protocolos de las capas adyacentes sin ninguna restricción.

Además de esto, MPLS ofrece adaptación total a IP. Esto es de gran importancia porque actualmente el mundo se mueve con este protocolo. Con MPLS ganamos en muchos aspectos en los que ATM presentaba carencias. Gracias al label switching, técnica usada en MPLS para enrutar paquetes, conseguimos hacer este enrutado a más velocidad, a la vez que disminuimos el retardo y el jitter. Estas características son de especial interés en las redes troncales, donde uno de sus principales objetivos es enviar paquetes de una localización a otra en el mínimo tiempo posible. Pero MPLS va más allá que la velocidad y nos ofrece otras grandes ventajas como la posibilidad de tener el control de la ruta, asignar distintos anchos de banda a los enlaces o crear prioridades para la utilización de un enlace. Todas estas ventajas y otras constituyen lo que se llama Traffic-Engineering (TE) y que suele designarse como MPLS-TE.

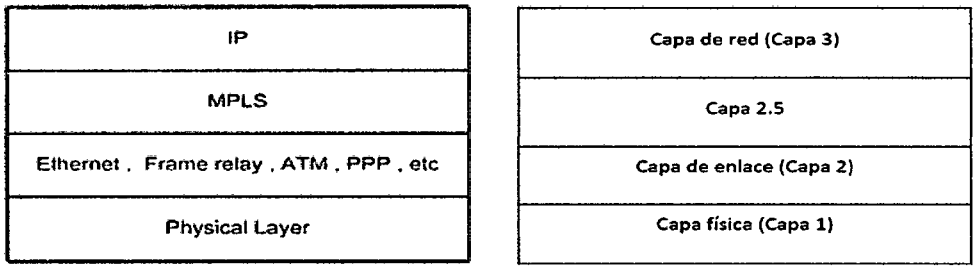


Fig. 2.11 Posición de MPLS en el modelo OSI[16]

Multi Protocol Label Switching está reemplazando rápidamente frame relay como la tecnología preferida para llevar datos de alta velocidad y voz digital en una sola conexión. MPLS no sólo proporciona una mayor fiabilidad y un mayor rendimiento, sino que a menudo puede reducir los costos generales mediante una mayor eficiencia de la red. Su capacidad para dar prioridad a los paquetes que

[16] Tomado de: http://upcommons.upc.edu/pfc/bitstream/2099.1/11730/1/PFC.pdf

transportan tráfico de voz hace que sea la solución perfecta para llevar las llamadas VoIP.

Debemos considerar MPLS como el avance más reciente en la evolución de las tecnologías de routing y forwarding en las redes IP, lo que implica una evolución en la manera de construir y gestionar estas redes. Los problemas que presentan las soluciones actuales de IP sobre ATM, tales como la expansión sobre una topología virtual superpuesta, así como la complejidad de gestión de dos redes separadas y tecnológicamente diferentes, quedan resueltos con MPLS. Al combinar lo mejor de cada nivel (la inteligencia del routing con la rapidez del switching) en un único nivel, MPLS ofrece nuevas posibilidades en la gestión de backbones, así como en la provisión de nuevos servicios de valor añadido.

2.4 Programa GNS3

GNS3 es un simulador gráfico de red que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos. Con GNS3 está ejecutando un Cisco IOS real, por lo que verá exactamente lo que el IOS produce y tendrá acceso a cualquier comando o parámetro con el apoyo del IOS, el cual se asemeja a ser lo más cerca posible a la forma real de los equipos que utilizan para implementación de redes como son los routers switches, etc. Para permitir completar simulaciones, GNS3 está estrechamente vinculada con:

- Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios imágenes IOS de Cisco Systems.
- Dynagen, un front-end basado en texto para Dynamips
- Qemu, un emulador de PIX.GNS3 es una excelente herramienta complementaria a los verdaderos laboratorios para los administradores de redes.[17]

Fig. 2.12 Modo de funcionamiento de la Plataforma GNS3

[17] Tomado de: http://www.gns3.net/

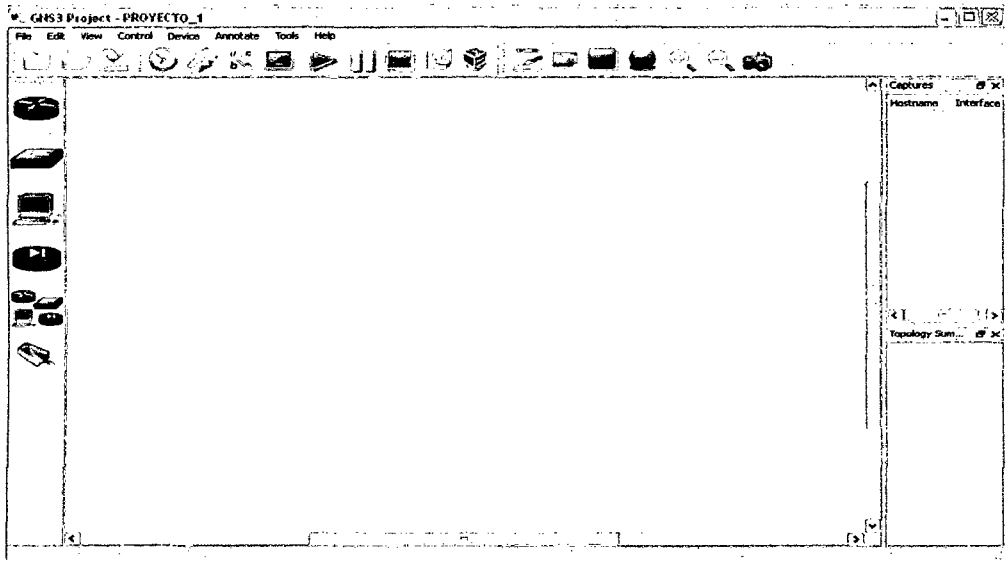


Fig. 2.13 Entorno de trabajo del programa GNS3.[18]

2.5. JPERF

Jperf es una herramienta de distribución libre, capaz de medir el ancho de banda, el retardo, el Jitter e incluso la pérdida de paquetes de un enlace entre dos PCs. Sus principales característica recaen en la facilidad con la que permite configurar sus diferentes parámetros, ya que posee una interfaz gráfica escrita en Java, es la interface gráfica del Iperf y tiene la capacidad de poder enviar datos que usan tanto el protocolo TCP, como el protocolo UDP.

Jperf trabaja bajo el modelo de cliente-servidor, en donde el PC cliente inventa información sin sentido que intenta mandar a otro PC que actúa como servidor durante un tiempo determinado, para ello el cliente necesita saber la dirección IP del PC servidor. Básicamente el cliente es el que envía la información y el servidor es el que registra los datos que obtiene cuando le llegan los paquetes y los muestra.

[18] Tomado de: http://www.gns3.net/

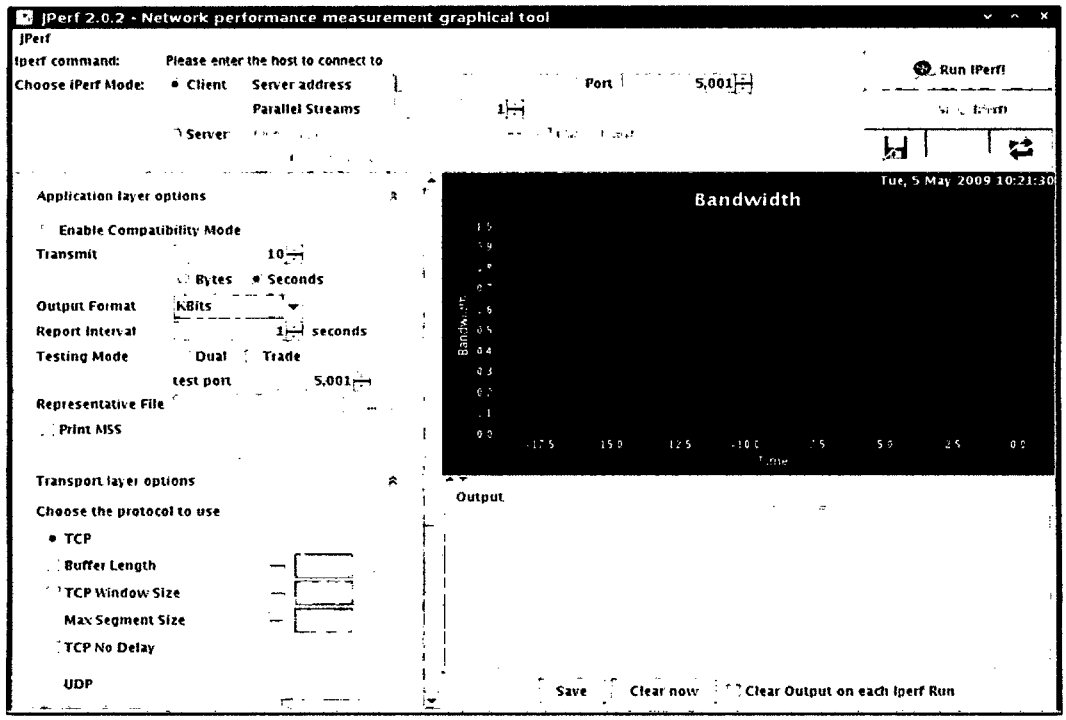


Fig. 2.14 Entorno de trabajo del JPERF[19]

[19] Tomado de: http://seguridadyredes.wordpress.com/2009/10/23/jperf-el-frontend-grafico-de-iperf-rendimiento-de-la-red/

CAPITULO III

HERRAMIENTA GNS3

3.1 Requerimiento del sistema

Se realizó un análisis comparativo entre las maquinas a utilizar para garantizar un buen rendimiento del emulador. Observando así el consumo de requisitos al momento de emular diversos routers.

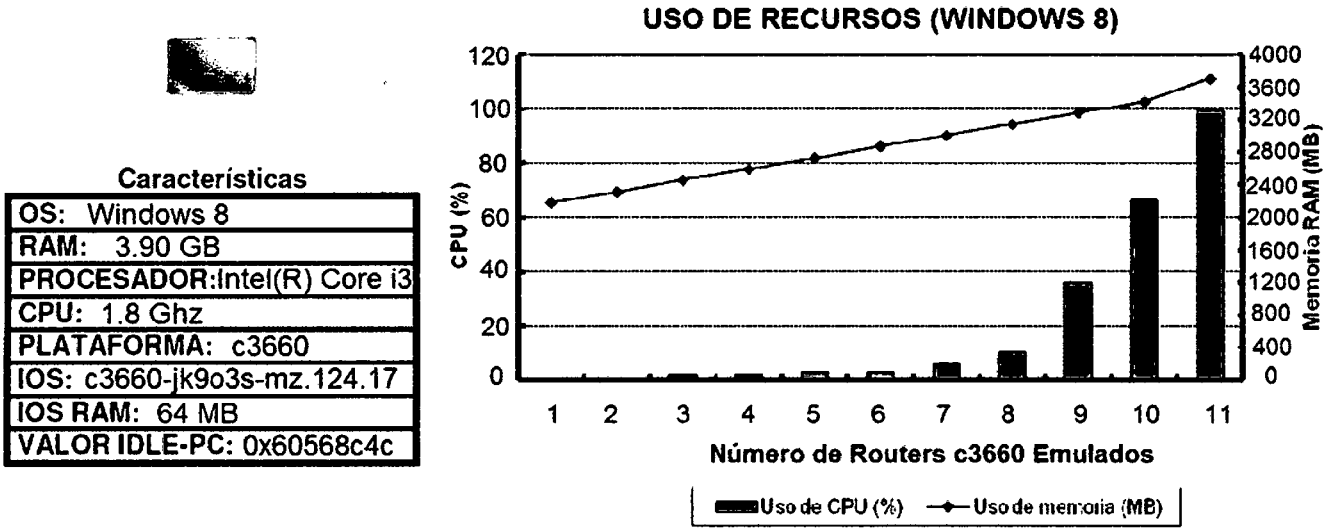


Fig. 3.1 Uso de recursos de maquina 1

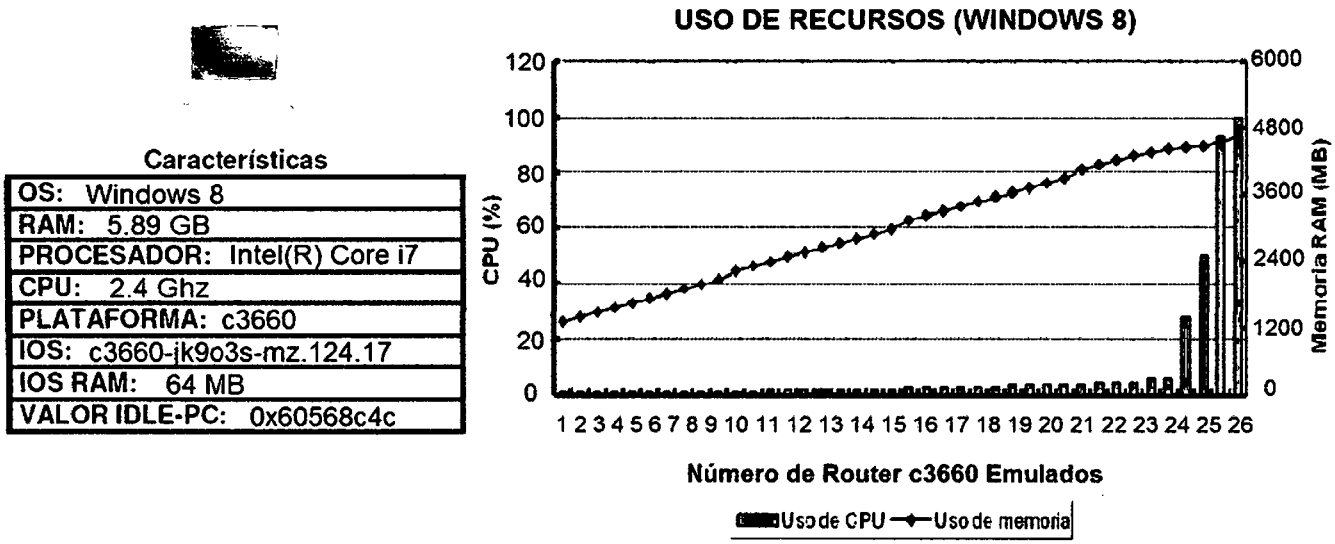


Fig. 3.2 Uso de recursos de maquina 2

3.2 Instalación y configuración en Windows 8.

3.2.1 Descargar el archivo de instalación

El primer paso para la instalación es descargar el archivo, GNS3-0.8.7-all-in-one.exe (ocupa aproximadamente 38.5 MB), que se encuentra en la página web http://www.gns3.net/download/.

El archivo anterior contendrá la versión binaria de los siguientes programas:

Dynamips 0.2.10 – Dynagen 0.11.0: Ambos programas son la base para el funcionamiento de GNS3.

Pemu 0.2.3: Es un emulador de firewalls PIX de Cisco basado en QEMU que no es más que una máquina emuladora y virtualizadora de código libre.

WinPcap 4.1.11: Permite la comunicación de redes virtuales con redes reales, ya que se encarga de detectar las interfaces reales del PC de trabajo para que el simulador pueda asignarlas como extremo de un enlace hacia un router virtual.

Wireshard 1.10.2 es un analizador de paquetes y protocolos de red. Se utiliza para la resolución de problemas, el análisis y el desarrollo de la red.

3.2.2 Instalar GNS3

En esta sección, una vez se haya dado doble clic al archivo que acaba de descargar, los sucesivos cuadros de diálogo lo guiarán durante el proceso de instalación de forma habitual.

La mayoría de los valores que aparecen por defecto son los que aceptaremos en la instalación, a no ser que se desee cambiar el directorio donde se instalará el simulador GNS3.

Los pasos para la instalación son los siguientes:

1) Dar doble clic al archivo de instalación descargado anteriormente. Nos aparecerá una ventana como la que se muestra en la figura 3.3 Hacer clic en "Next".
2) Aceptar la licencia haciendo clic en el botón "I Agree" como se observa en la figura 3.4.

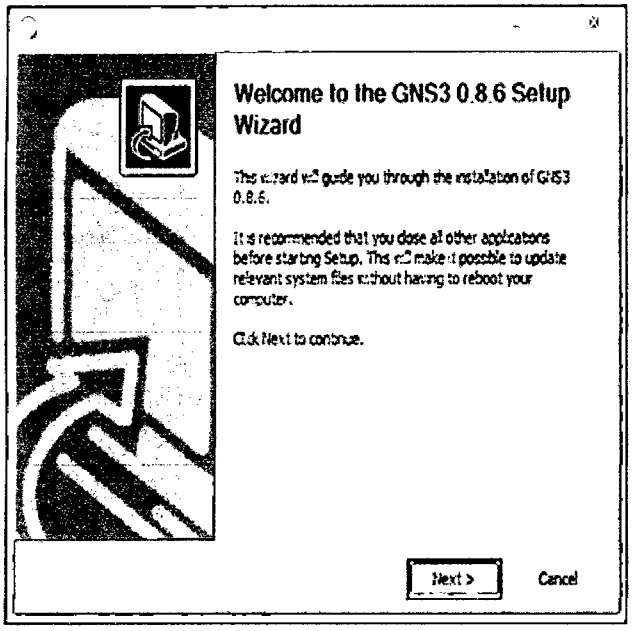


Fig. 3.3 Iniciar instalación del GNS3.

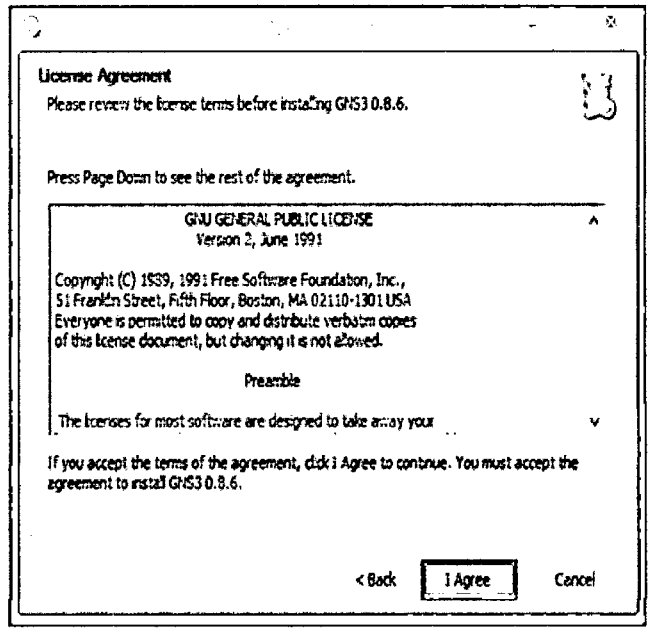
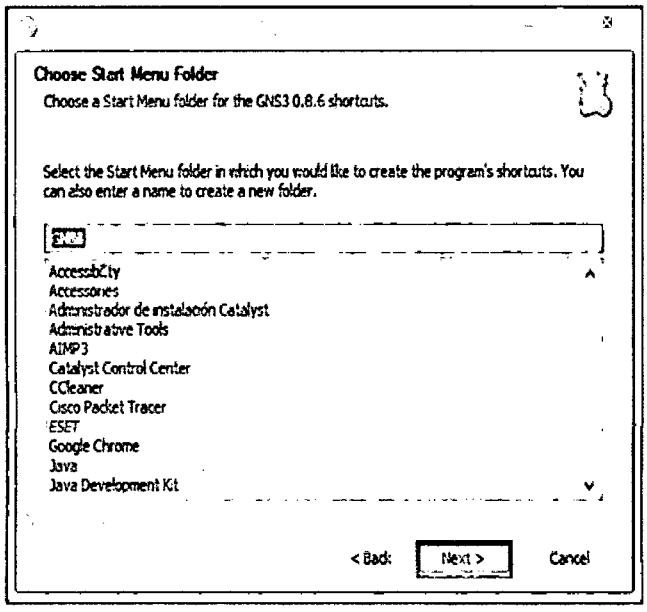


Fig. 3.4 Aceptar Lincense Agreement.

3) Indicar el nombre del directorio de inicio de GNS3. Seguidamente hacer clic en "Next". Ver figura 3.5
4) Aceptar todos los componentes que se instalarán por defecto. Hacer clic en "Next". Ver figura 3.6



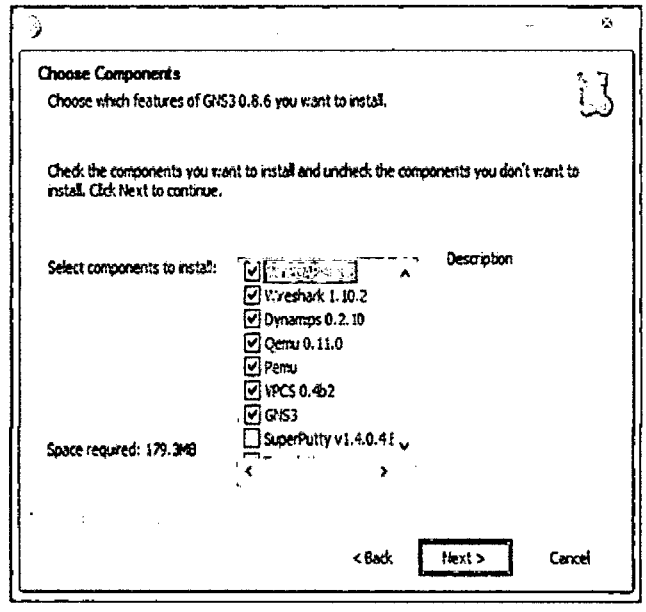


Fig.3.5 y Fig. 3.6: Proceso de instalación del GNS3.

5) En la figura figura 3.7, Indicar la ubicación del directorio donde se instalará al simulador. Seguidamente hacer clic en "install".

6) Antes de concluir la instalación de GNS3, aparecerá la ventana que da inicio a la instalación de WinPcap como se muestra en la figura 3.9. Hacer clic en "Next".

7) Aceptar la licencia de WinPcap haciendo clic en "I Agree". Ver figura 3.10.

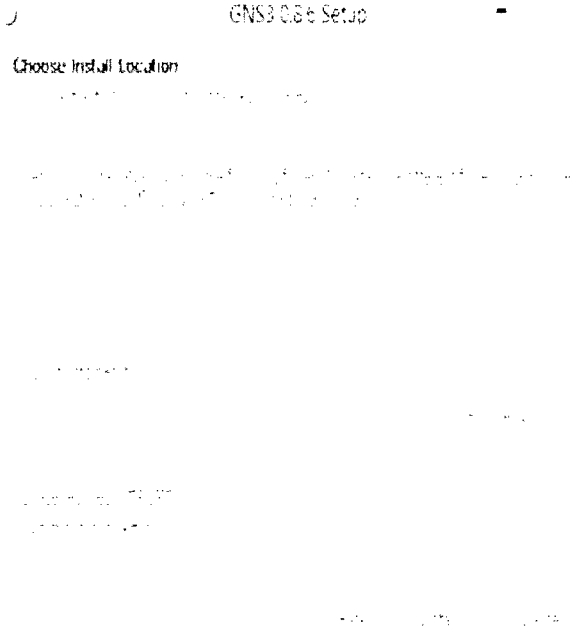


Fig. 3.7 Carpeta de destino.

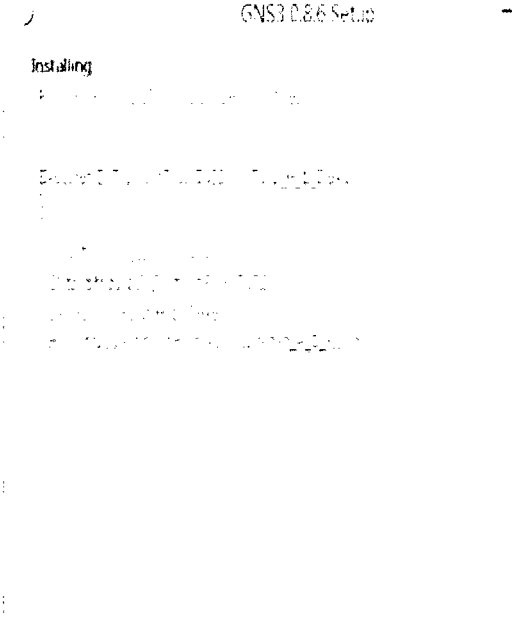


Fig. 3.8 Ejecutando instalador de WinPcap.

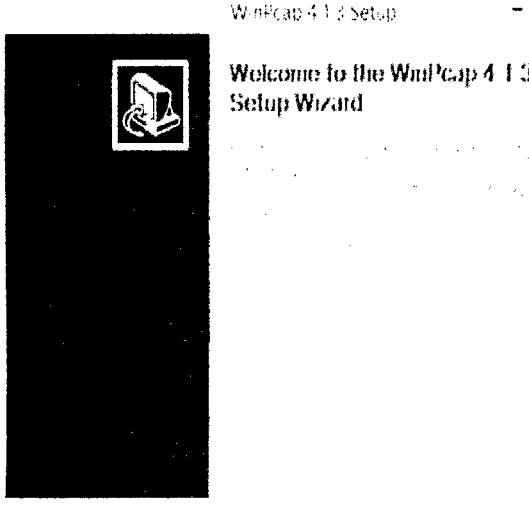


Fig. 3.9 Instalar WinPcap.

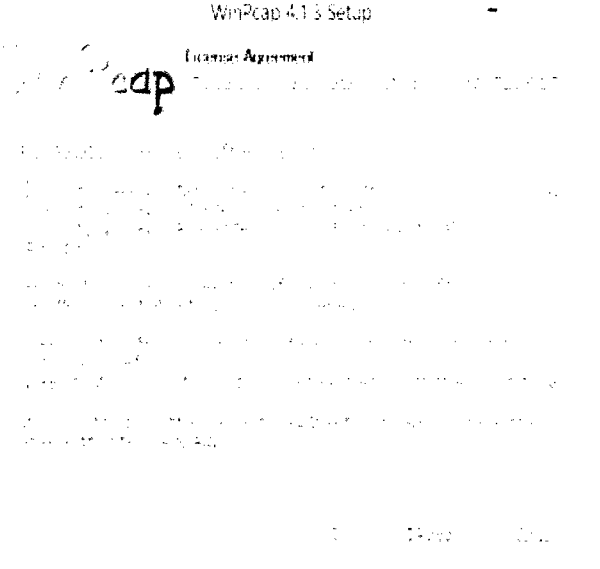


Fig. 3.10 Aceptar License Agreement.

8) Después de la instalación de WinPcap, aparecerá la ventana que da inicio a la instalación de Wireshark como se muestra en la figura 3.11.

9) Aceptar la licencia de Wireshark haciendo clic en "I Agree". Ver figura 3.12

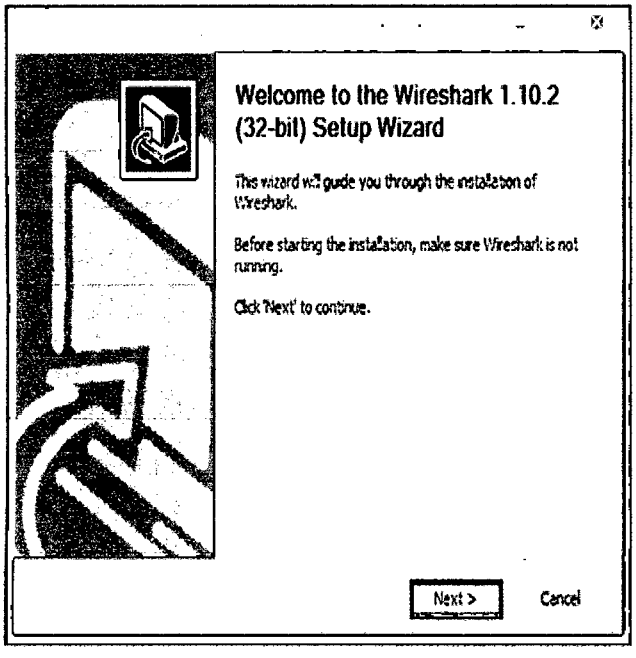


Fig. 3.11 Instalar Wireshark

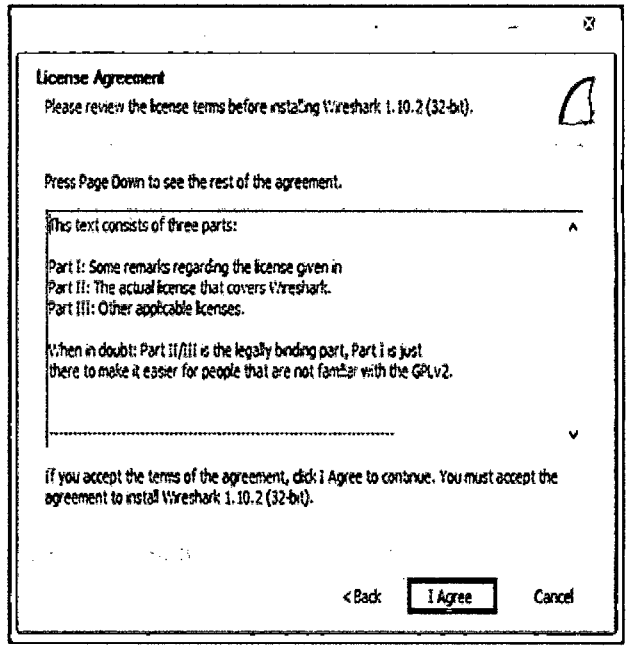
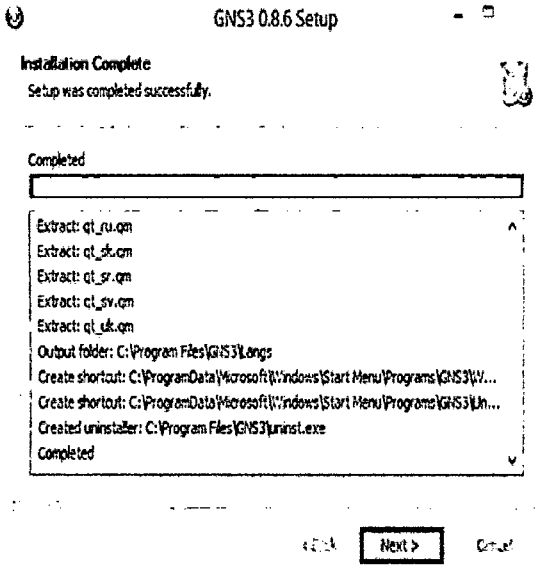


Fig. 3.12 Aceptar License Agreement.

10) Una vez acabada la instalación del Wireshark se retomará la instalación de GNS3 y cuando ésta termine aparecerá una ventana como en la figura 3.13. Hacer clic en "Next" y luego en "Finish" para terminar la instalación.



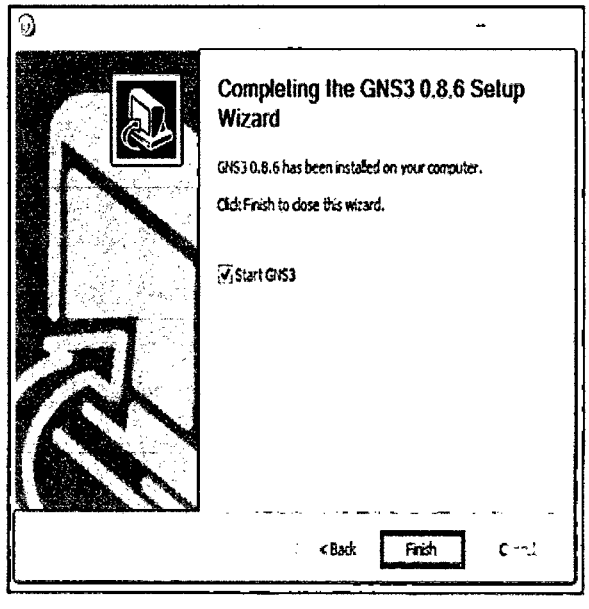


Fig. 3.13 y Fig.3.l4: Finalización de instalación del GNS3

11) Tras la finalización de la instalación, podemos ejecutar la aplicación desde "Programas" en el menú de "Inicio" o haciendo doble click en el icono correspondiente del escritorio, y aparecerá la pantalla de la figura 3.15.

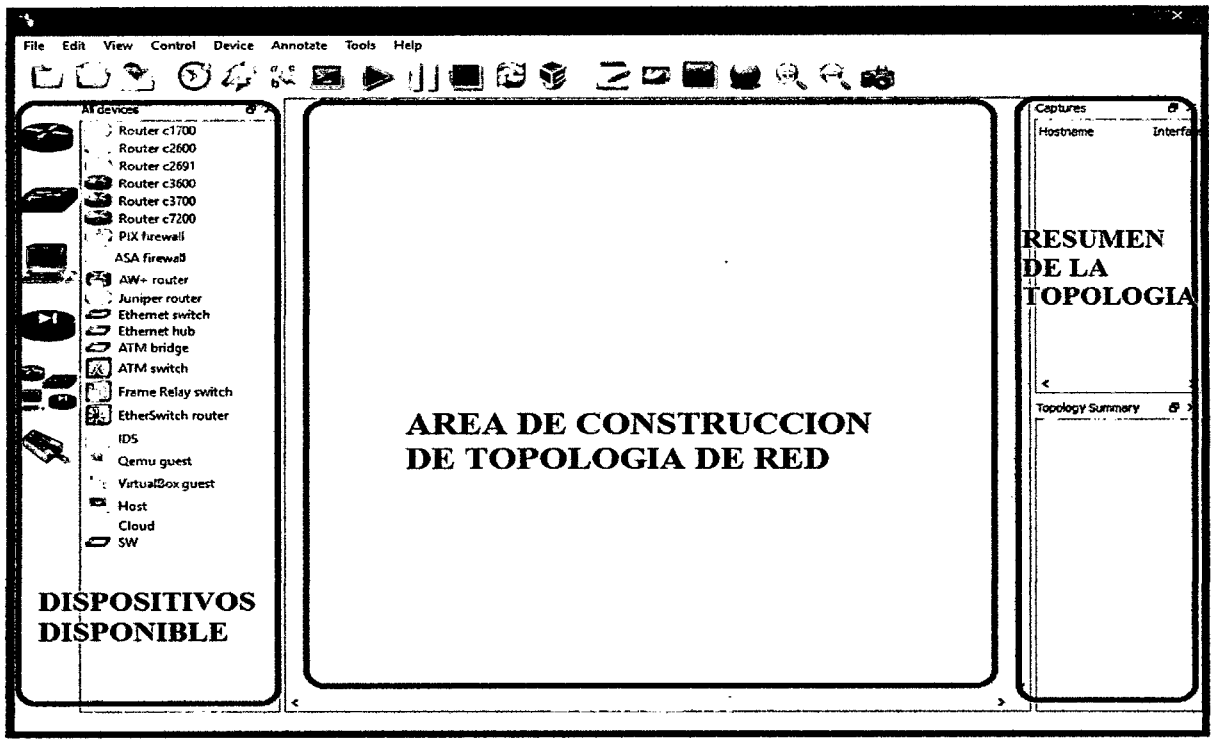


Fig. 3.15 Ventana de GNS3 en Windows 8.

3.2.3 Comprobar el path hacia Dynamips

Una vez instalado GNS3 es importante comprobar si el simulador ha podido reconocer de forma eficaz el path donde se encuentra instalado Dynamips para que pueda usarlo correctamente. Los pasos para realizar esta tarea son los siguientes:

1) En la aplicación, seleccionar la opción "Preferences" del menú Edit, como se muestra en la figura 3.16.

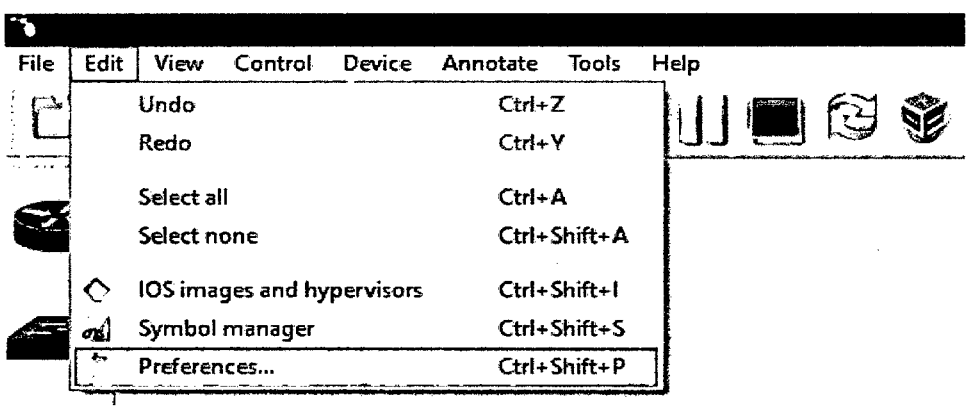


Fig. 3.16 Inicio para la comprobación del path del Dynamips

2) Cuando aparece la ventana de "Preferences" indicamos la ubicación donde se van a guardar los proyectos realizados en el GNS3 y la ubicación donde se encuentran las imágenes IOS de CISCCO que utilizaron los equipos virtuales en las topologias implementadas.
3) Una vez indicadas correctamente las ubicaciones hacer click en "Apply" para guardarlas, como se muestra en la Fig. 3.17

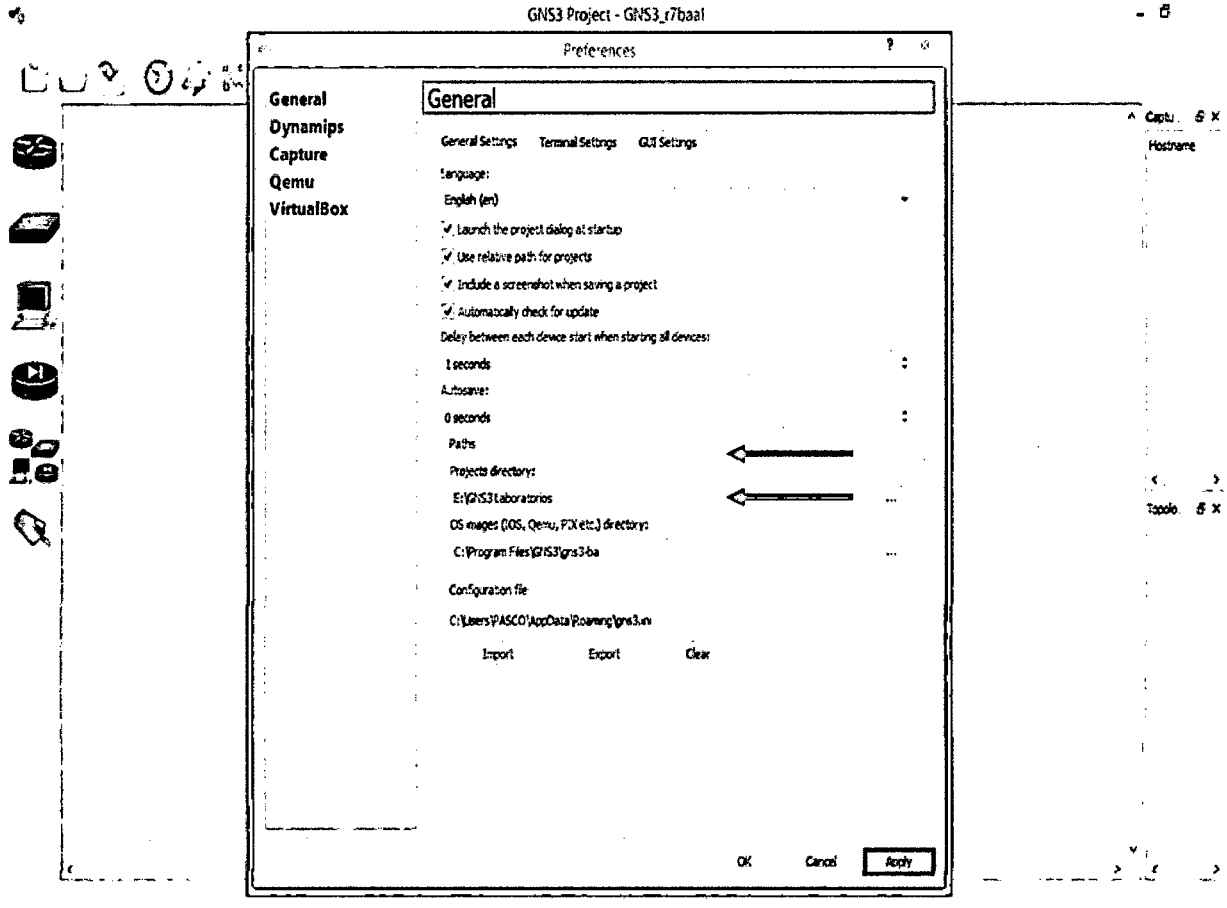


Fig. 3.17 Ventana General de Preferences.

4) En la misma ventana que ha aparecido hacer un clic sobre "Dynamips" para obtener la pestaña donde se muestra la ubicación de Dynamips. Comprobar que el path que se muestran es correcto haciendo clic en "Test", cuando aparece el mensaje "Dynamips succesfuly started" a un costado significa que el GNS3 ha sido instalado correctamente y esta lsito para usarce, si obtenemos algún error buscar la verdadera ubicación Dynamips. No olvidar comprobar que se encuentran habilitadas las funciones de Ghostios, Sparsemem y mmap.

5) Por ultimo Hacer clic en "Apply" para guardar los datos.

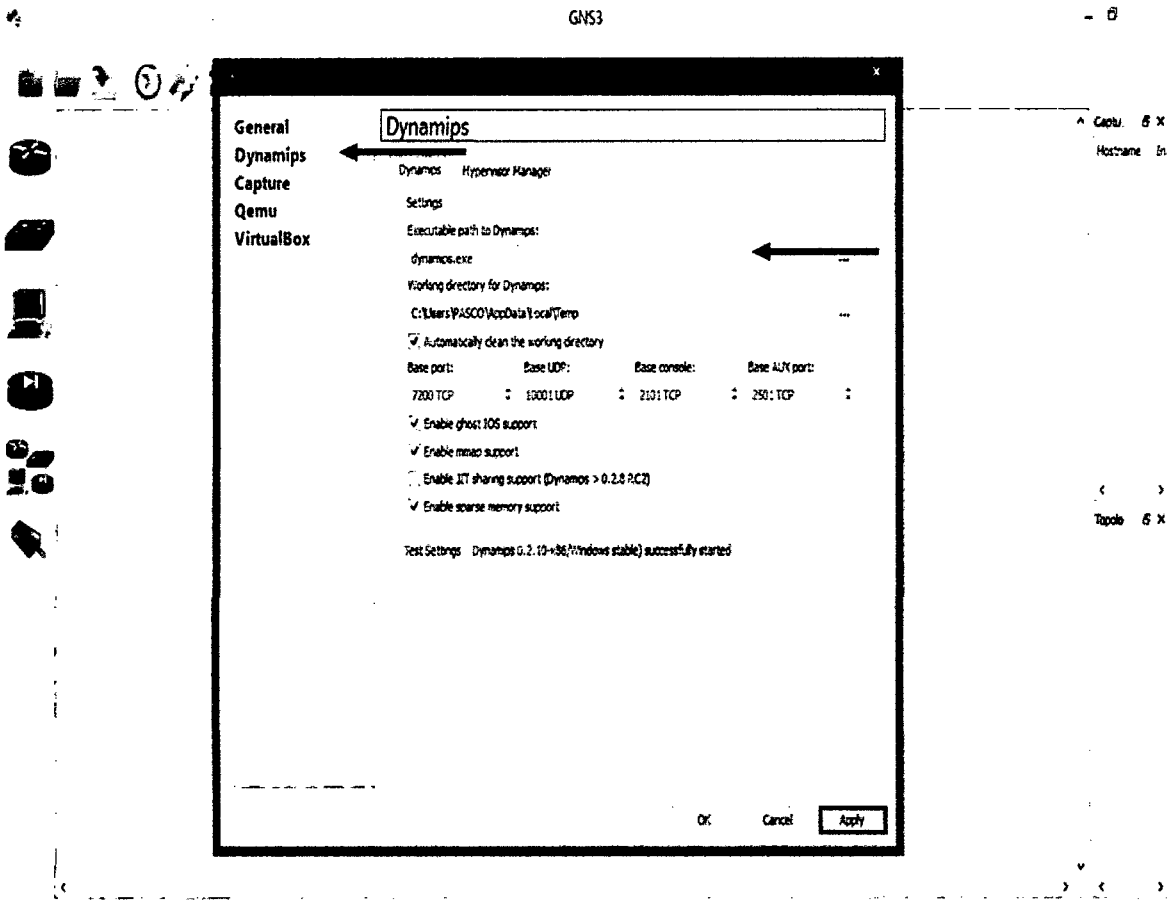


Fig. 3.18 Comprobación del path del Dynamips.

3.2.4 Cargar CISCO IOS

3.2.4.1. Cargar CISCO IOS Router.

El siguiente paso es la carga de la imagen IOS que usarán los routers virtuales de nuestra topología, para lo cual realizaremos los siguientes pasos:

1) Ejecutar la aplicación y seleccionar "IOS images and hypervisors" en el menú Edit, como se muestra en la figura 3.19.

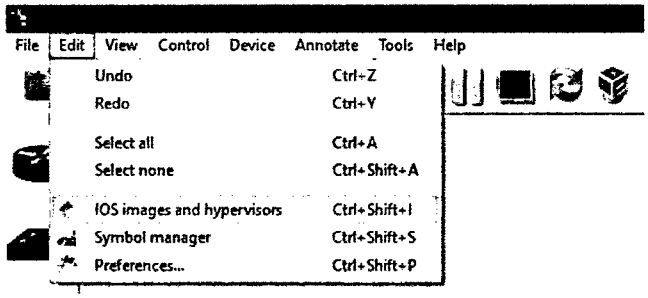


Fig. 3.19 Carga de los CISCO IOS Router en el GNS3

2) En la ventana que aparece, buscar la ubicación de la imagen IOS en el PC. Ver la figura 3.20

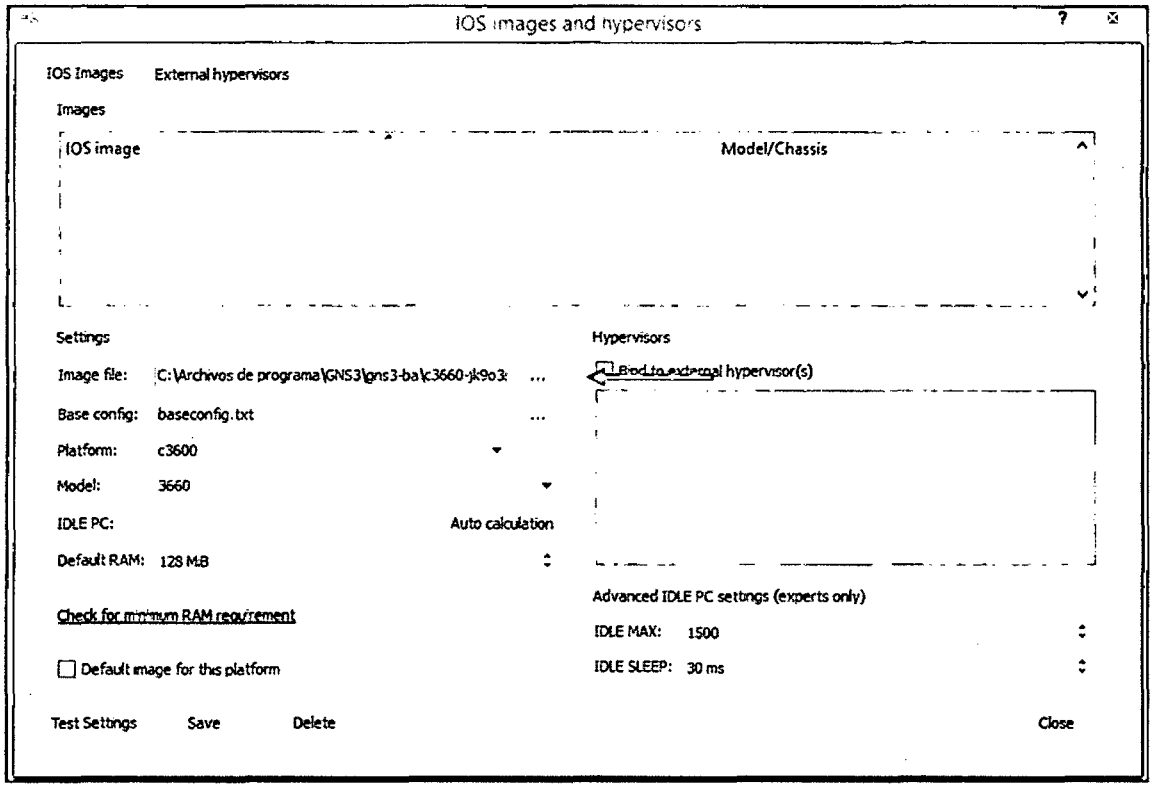


Fig. 3.20 Ubicación de CISCO IOS en el GNS3

3) Seguidamente elegiremos la plataforma y el modelo que corresponde con la imagen IOS que usaremos para simular, para ello hacer clic sobre Más adelante se mostrará la manera de asignar valores de IDLE PC al router y de cambiar los valores de memoria RAM del mismo.

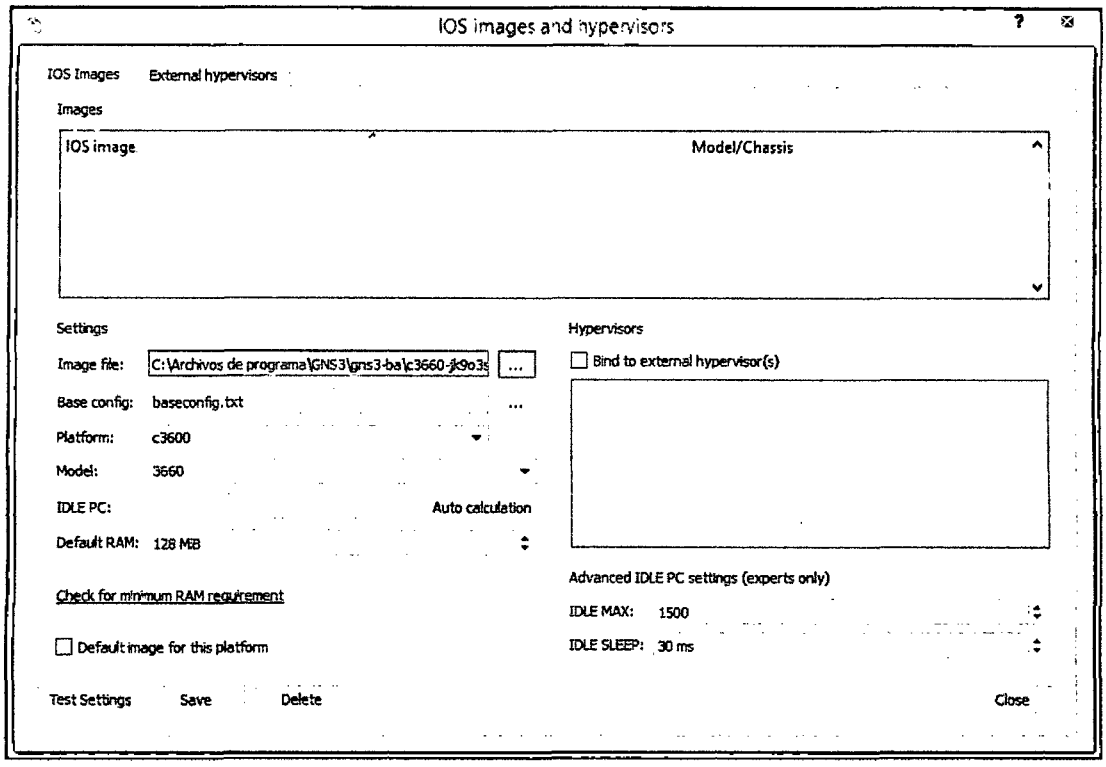


Figura 3.21 Selección de CISCO IOS en el GNS3

4) Finalmente guardamos los cambios haciendo clic en "Save" y después en "Close". Notar que el valor de IDLE-PC se encuentra vacío por el momento.

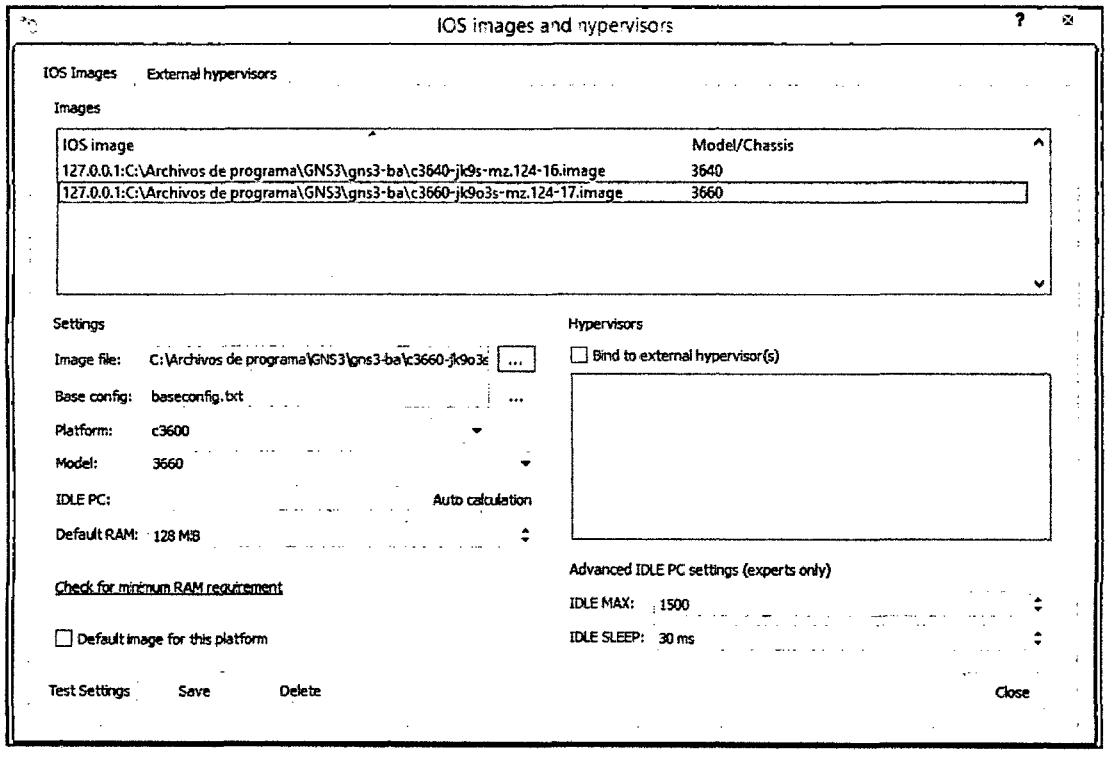


Fig. 3.22 Almacenamiento de CISCO IOS en el GNS3

3.2.4.2. Cargar CISCO IOS ASA FIREWALL.

Antes de realizar la configuración se deberá descargar los dos siguientes archivos: asa842-initrd y asa842-vmlinuz.

Seguir los siguientes pasos para cargar ASA FIREWALL:

1) Seleccionar la opción "Preferences" del menú Edit, como se muestra en la figura.

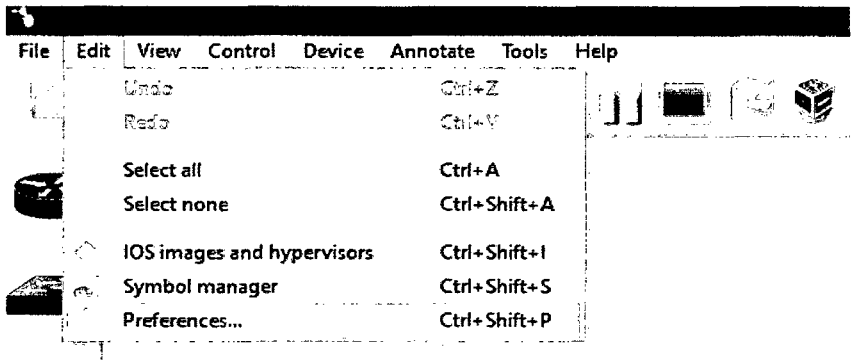


Fig. 3.23 Carga de los CISCO IOS ASA FIREWALL en el GNS3

2) Luego seleccionar Qemu y seguidamente la pestaña ASA, como se muestra la figura.

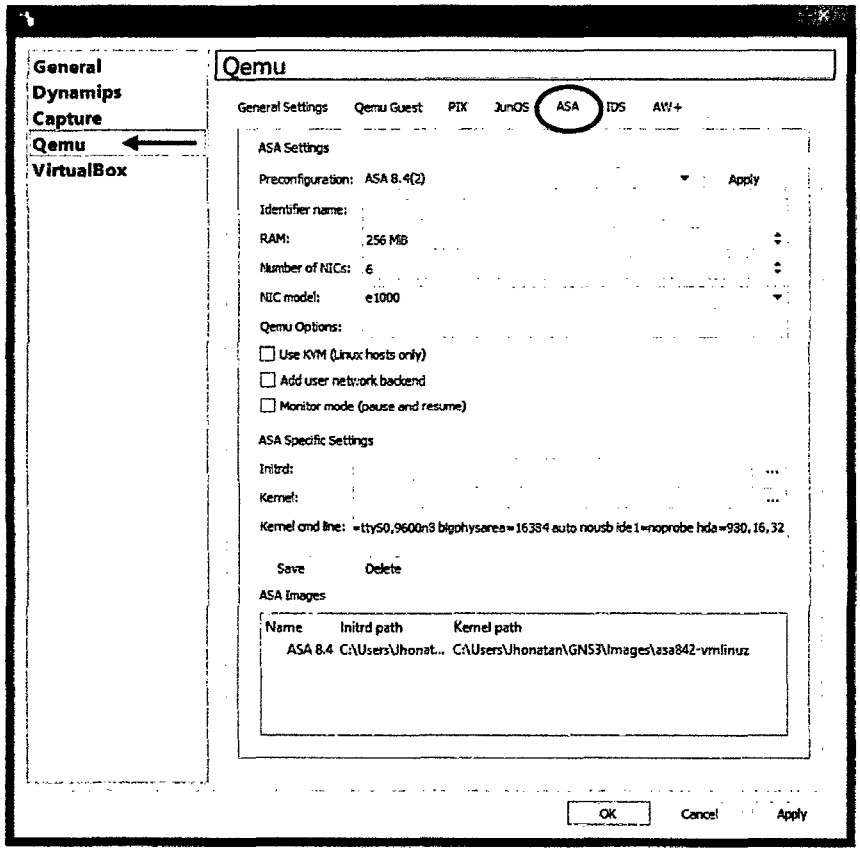


Fig. 3.24 Ventana Qemu en GNS3.

3) Buscar los dos archivos previamente descargados en el área de ASA Specific Settings:

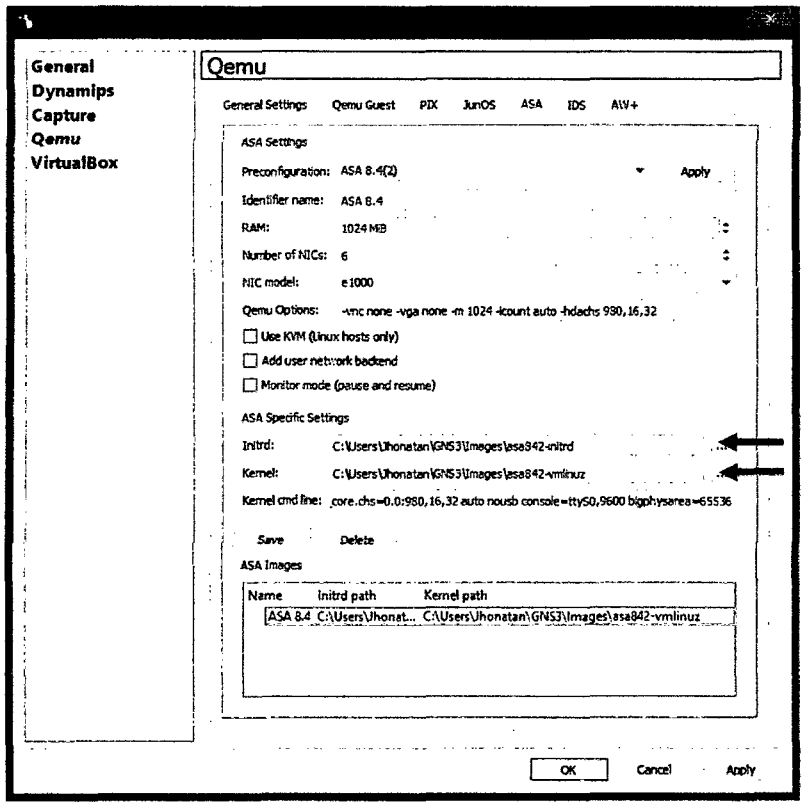


Fig. 3.25 Carga archivos descargados.

4) Se deberá copiar las líneas de código en las opciones:

Qemu Options: -vnc none -vga none -m 1024 -icount auto -hdachs 980,16,32

Kernel cmd line: -append ide_generic.probe_mask=0x01 ide_core.chs=0.0:980,16,32 auto nousb console=ttyS0,9600 bigphysarea=65536

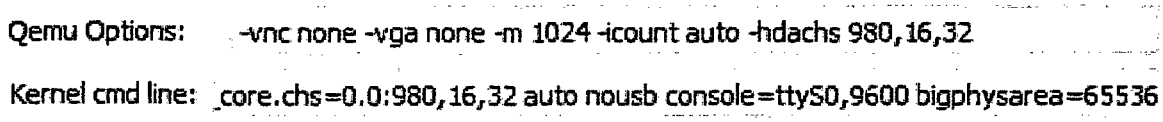


Fig. 3.26 Modificar líneas de códigos.

5) Luego clic en "Save".

6) Seguidamente clic en "Apply" y finalmente en "OK".

3.2.4.3. Cargar CISCO IOS Switch.

En realidad se utiliza un router cisco de la gama 3700 como un switch con el módulo NM-16ESW. Este módulo proporciona al router un switch de 16 puertos, con lo que nos permite trabajar con algunas características como pueden ser las vlan, trunk, vtp, port aggregation o EherChannel, port mirroring, etc.

Seguir los siguientes pasos:

1) Primero cargar la imagen CISCO IOS.

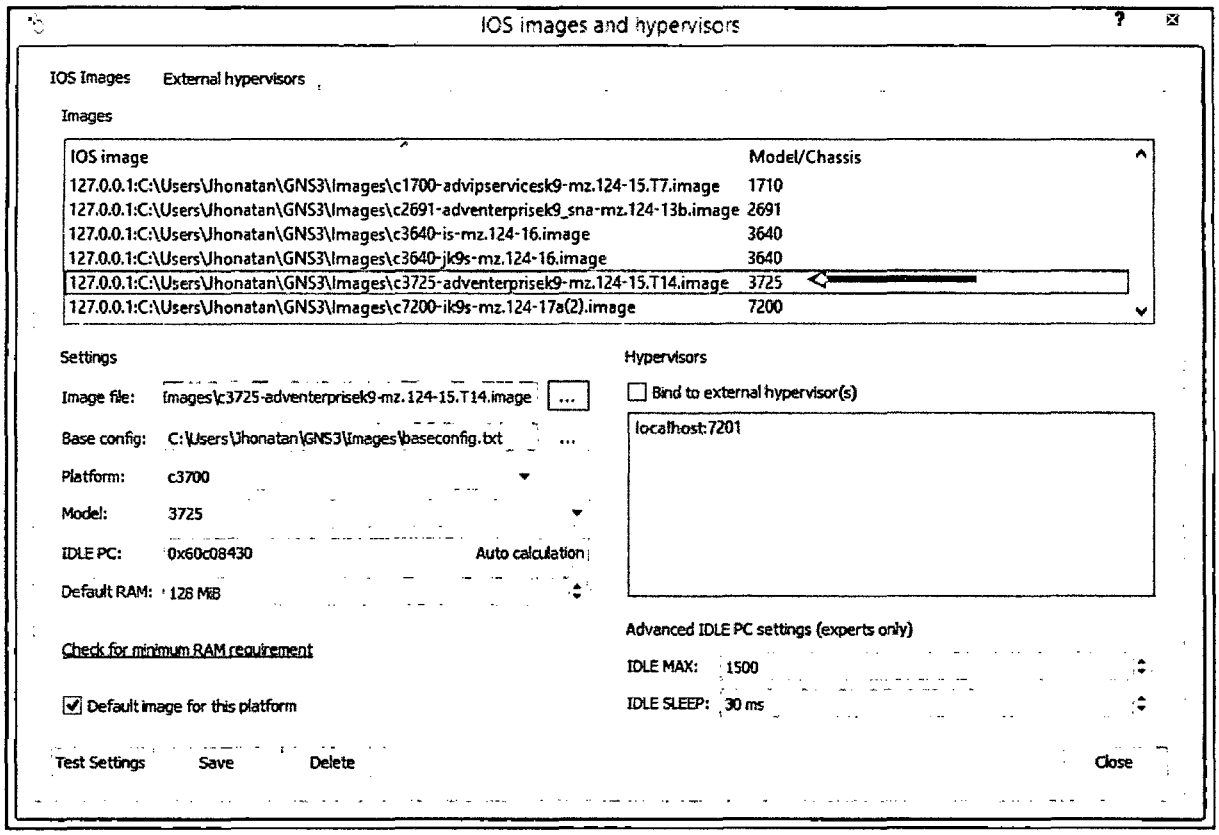


Fig. 3.27 Cargar CISCO IOS.

2) Seleccionar "Symbol manager" del menú "Edit".

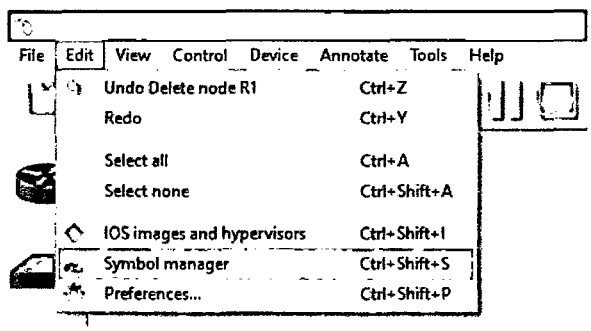


Fig. 3.28 Selección de Symbol manager.

3) Escoger una imagen y clic en ">" para agregarlo en el área de dispositivos disponibles.

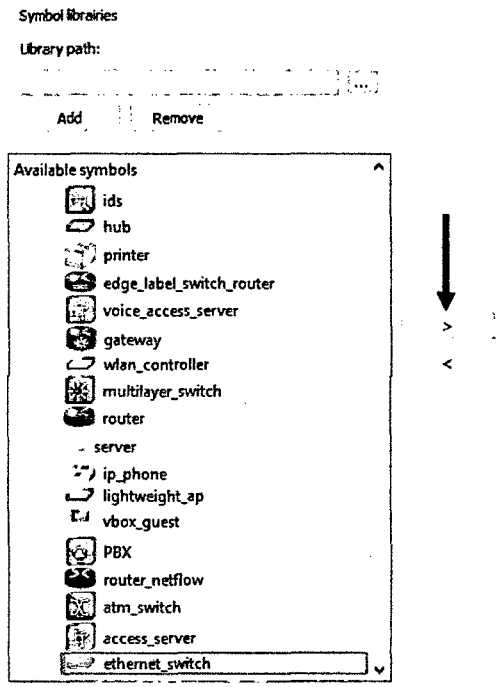


Fig. 3.29 Escoger imagen.

4) Asignar un nombre y seleccionar en type: Router c3700 y finalmente clic en "OK".

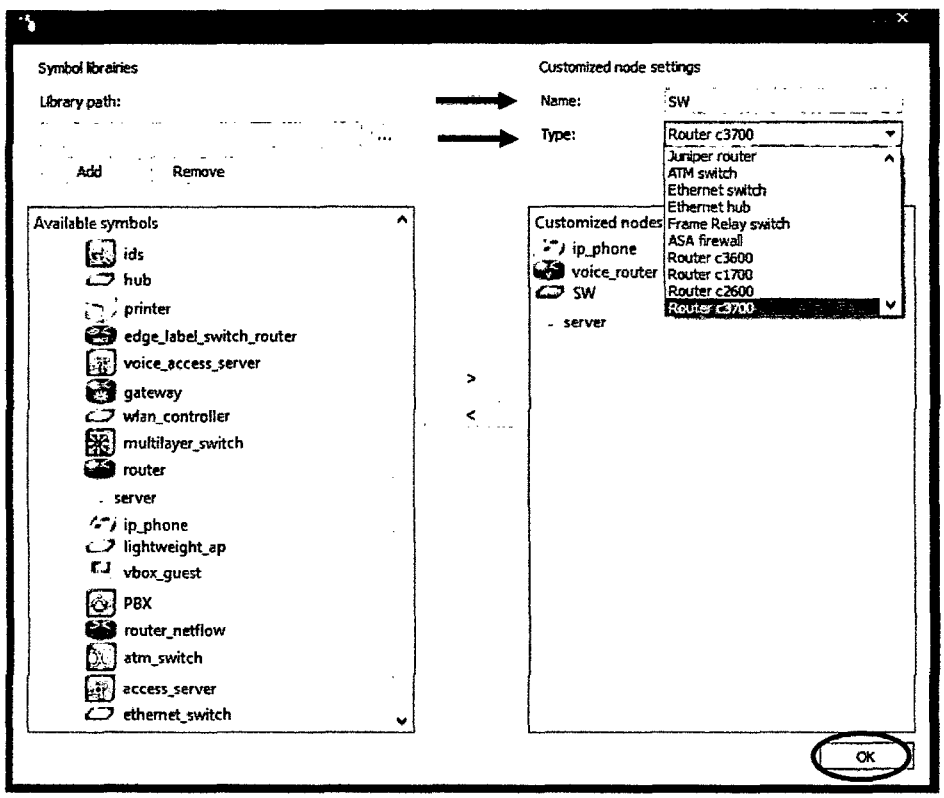


Fig. 3.30 Configurar Symbol Manager.

3.3 Uso del GNS3

3.3.1 Emulación de Routers CISCO.

Para emular los routers CISCO se necesitan una imagen CISCO IOS. En ese sentido el emulador habilitara un número de ranuras y slots dependiendo del tipo de plataformas, en el siguiente cuadro se detalla más detenidamente.

Adaptador de interfaces disponibles		
Routers	**Nombre**	**Descripción**
1700s	WIC-1T	1 puerto serie
	WIC-2T	2 puertos serie
	WIC-1ENET	1 puerto Ethernet
2600s	NM-1E	puerto Ethernet
	NM-4E	4 puertos Ethernet
	NM-1FE-TX	1 puerto FastEthernet
	NM-16ESW	Módulo de switch Ethernet (16 puertos)
	NM-NAM	Conecta el router virtual a un PC virtual
	NM-IDS	Conecta el router virtual a un PC virtual
	WIC-1T	1 puerto serie
	WIC-2T	2 puertos serie
3600s	NM-1E	1 puerto Ethernet
	NM-4E	4 puertos Ethernet
	NM-1FE-TX	1 puerto FastEthernet
	NM-16ESW	Módulo de switch Ethernet (16 puertos)
	NM-4T	4 puertos serie
	Leopard-2FE	Puerto automático FastEthernet en slot 0
3700s	NM-1FE-TX	(FastEthernet, 1 port) 1 puerto FastEthernet
	NM-4T	4 puertos serie
	NM-16ESW	Módulo de switch Ethernet (16 puertos)
	GT96100-FE	2 puertos integrados
	NM-NAM	Conecta el router virtual a un PC virtual
	NM-IDS	Conecta el router virtual a un PC virtual
	WIC-1T	1 puerto serie
	WIC-2T 2	2 puertos serie
7200s	C7200-IO-FE	Solo puerto FastEthernet en slot 0
	C7200-IO-2FE	2 puertos FastEthernet en slot 0
	C7200-IO-GE-E	Solo Puerto GigabitEthernet en slot 0
	PA-FE-TX	1 puerto FastEthernet
	PA-2FE-TX	2 puertos FastEthernet
	PA-4E	4 puertos Ethernet
	PA-8E	8 puertos Ethernet
	PA-4T+	4 puertos serie
	PA-8T	8 puertos serie
	PA-A1	Puerto ATM
	PA-POS-OC3	Puerto POS
	PA-GE	1 puerto GigabitEthernet

Tabla 3.1 Adaptadores de interfaces disponibles

Los pasos a seguir para emulación y configuración de un router en GNS3 son los *siguientes:*

1) Hacer clic en el grupo de plataformas, seleccionar el router deseado a emular y arrastrar al área de construcción de topologías.

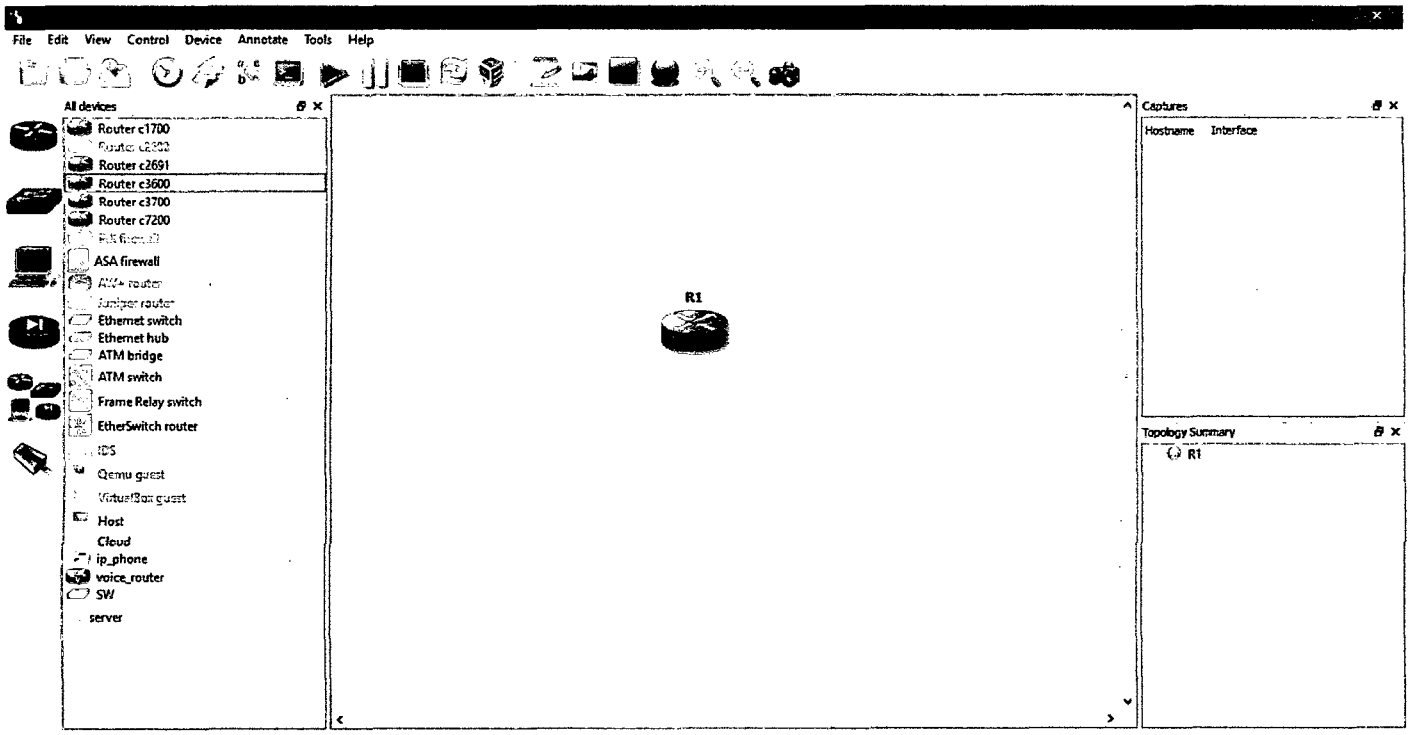


Fig. 3.31 Selección de router.

2) Hacer clic derecho sobre el router y elegir "configure"

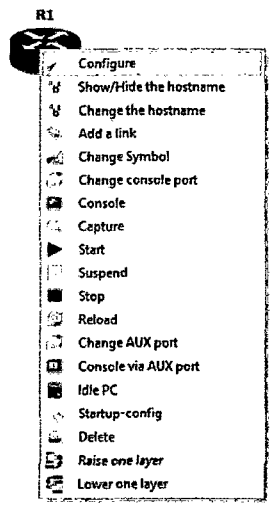


Fig. 3.32 Menú de opciones de router.

3) Hacer doble clic en el router, seleccionar el slots y elegir las interfaces que desea agregar, clic en Apply y luego en OK.

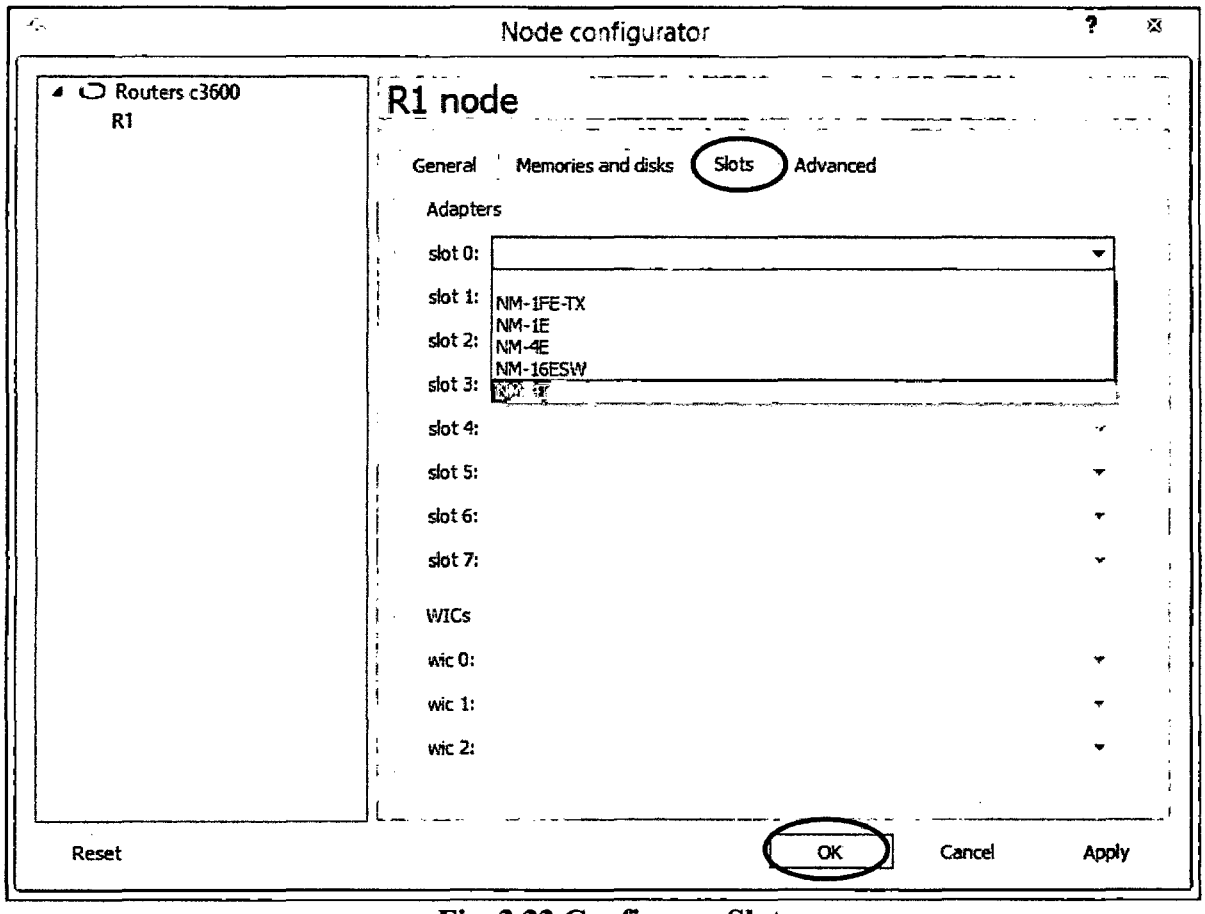


Fig. 3.33 Configurar Slots.

4) Clic derecho en el router y escoger "start" para encender el router.

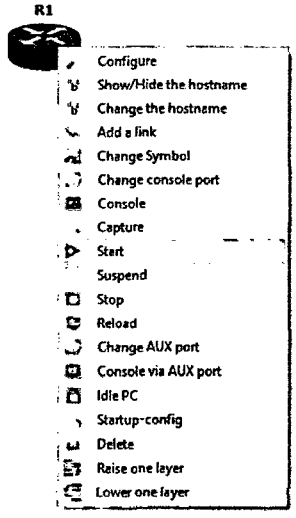


Fig. 3.34 Iniciar router.

5) Calcular el valor de IDLEPC para imagen IOS, haciendo clic derecho y eligiendo "Idle PC".

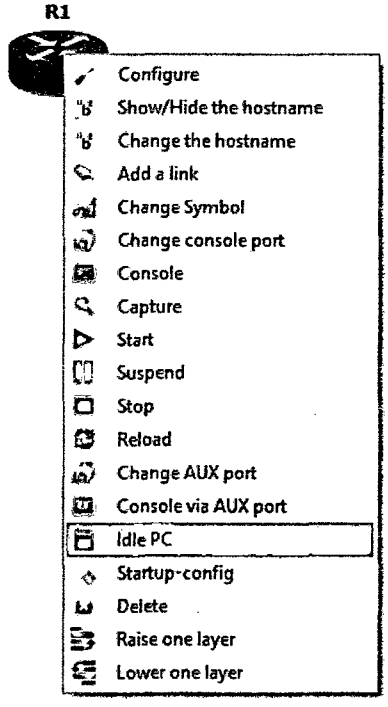


Fig. 3.35 Calcular IDLE PC.

6) Nos mostrara la siguiente ventana, seleccionar el valor que contenga el * y luego clic en "apply".

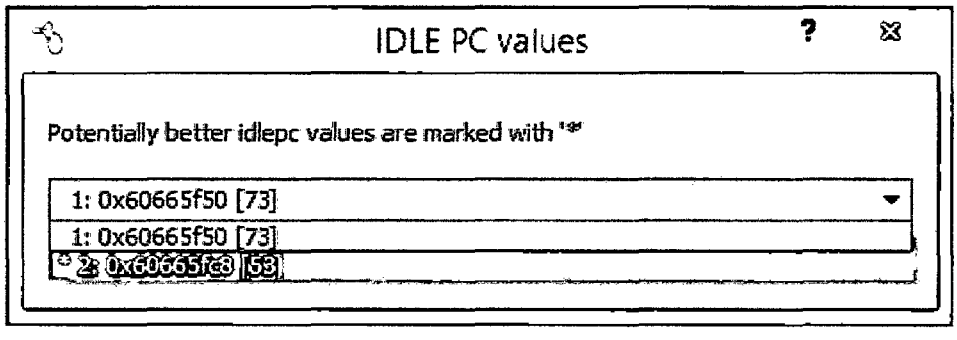


Fig. 3.36 Selección de IDLE PC.

7) Finalmente hacer clic derecho en el router y seleccionar "console" para poder ingresar a la ventana de configuración del router emulado.

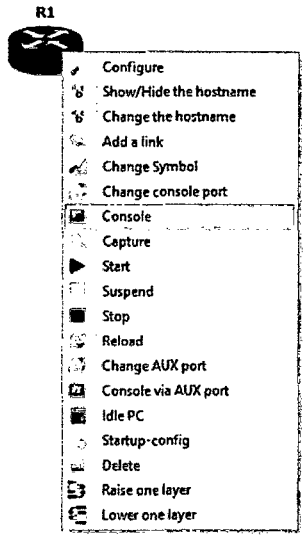


Fig. 3.37 Abrir console de configuración.

3.3.2 Emulación de Switch Ethernet

El software GNS3 también tiene la capacidad de emular switches Ethernet simples con funciones básicas como: Access, dot1q y qinq. Por defecto cada switch tiene 8 puertos access configurados en la Vlan1 pero se puede añadir hasta 10000 puertos.

Pasos para configurar switch Ethernet.

1) Seleccionar "Ethernet switch" y arrastrarlo hasta el área de construcción de topologías.

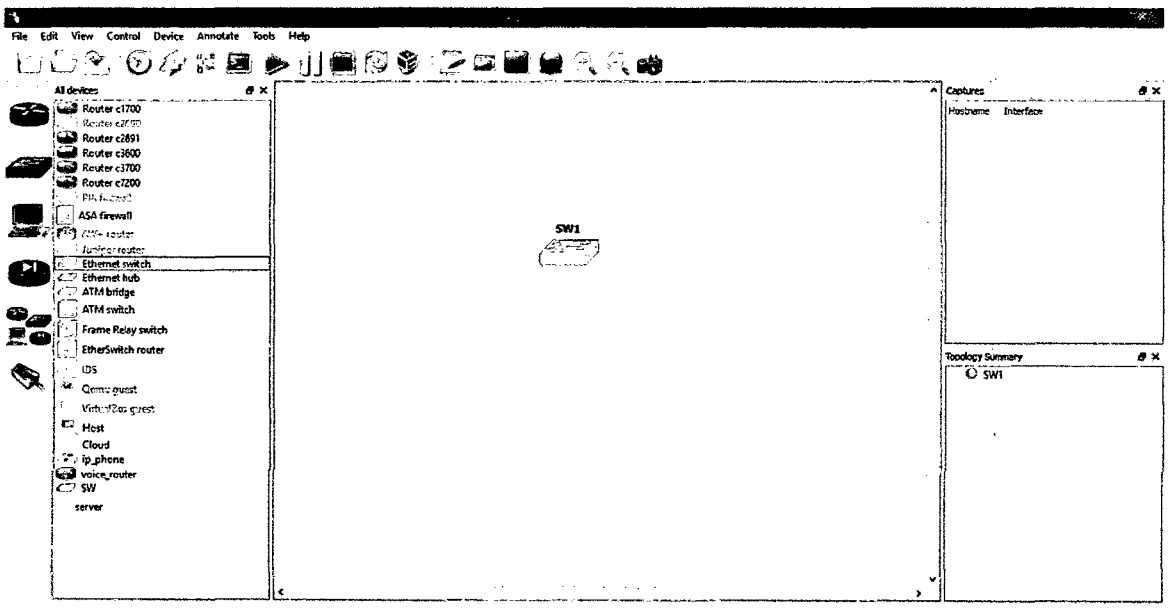


Fig. 3.38 Selección de Switch Ethernet.

2) Clic derecho en el switch y luego seleccionar "configure".

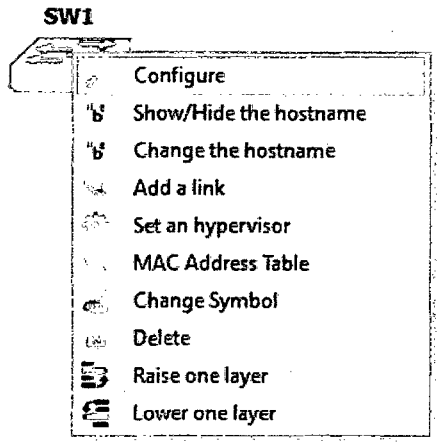


Fig. 3.39 Menú de opciones switch Ethernet.

3) Realizar las configuraciones deseadas

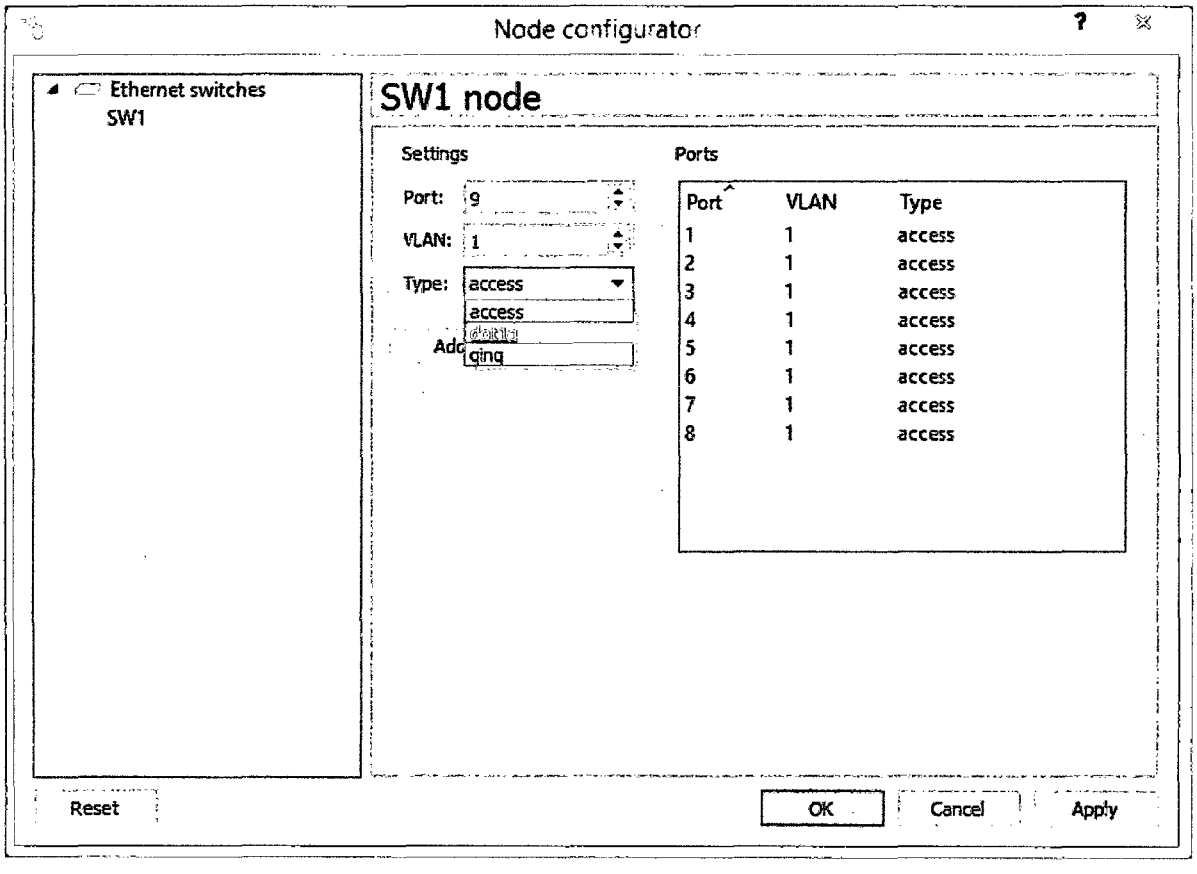


Fig. 3.40 Ventana de Configuración de nodo.

3.3.3 Simulación de PCs.

GNS3 también incorpora PCs, lo que facilita la comprobación y estudio de redes simuladas, gracias a las VPCS.

3.3.3.4 VPCS

Se puede simular hasta 9 ordenadores. Cada uno de ellos utiliza un par de puertos UDP para hablar y escuchar a los routers de Cisco que se ejecutan en el entorno GNS3. El Número de Virtual PC n (donde n = 0, 1,..., 8) escucha en el puerto UDP 20000 + n y espera a los Dynamips se conecten. Se envía los paquetes al puerto UDP 30000+ n. En GNS3 cada PC se representa como un servicio de nube con una interfaz NIO UDP (Entrada y salida de red para UDP) con puerto local 30000 + n y el puerto remoto 20000 + n.

Pasos para simular PCs:

1) Escoger el icono de Host y arrastrar al área de construcción de topologías.

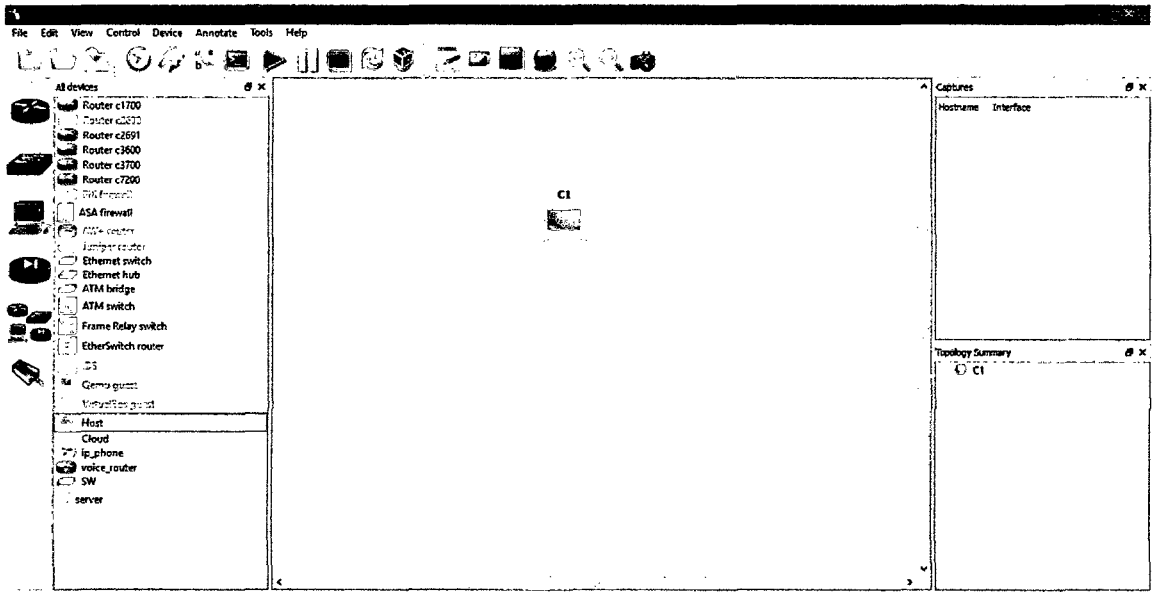


Fig. 3.41 Selección de VPCS.

2) Clic derecho en el host y seleccionar "configure".

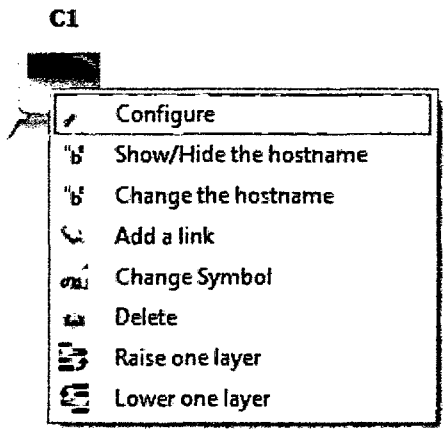
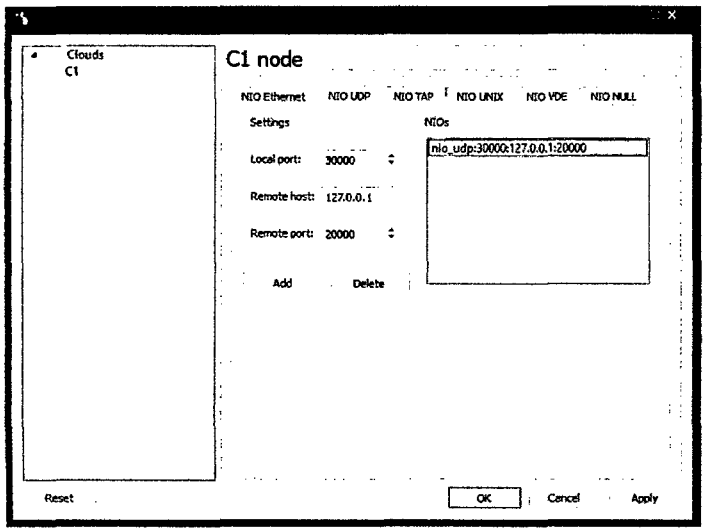


Fig. 3.42 Menú de opciones de VPCS.

3) Hacer clic en C1 y luego en "NIO UDP" y configurar parámetros "Local port" y "Remote port", para este caso C1 deberá tener en Local port: 30000 y Remote port: 20000, para C2 el Local port: 30001 y Remote port: 20001, etc.



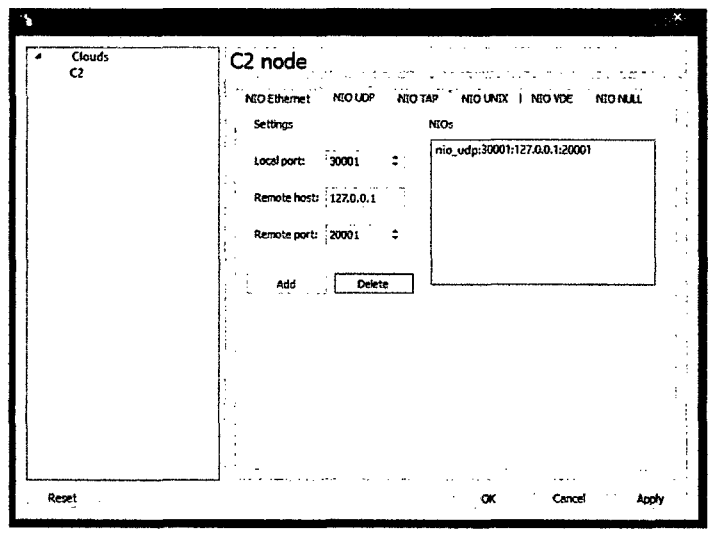


Fig. 3.43 y Fig. 3.44: Ventana de Configuración para VPCS.

4) Asignar IP a las VPCS.

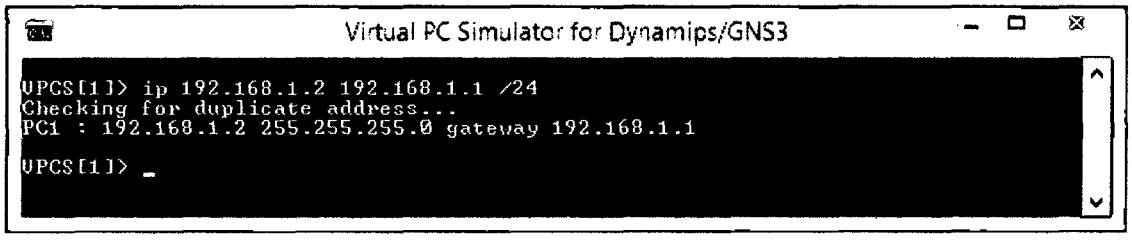


Fig. 3.45 Configurar IP para VCPS.

3.3.4 Enlace de equipos emulados.

El tipo de enlace dependerá del equipo emulado y que tipo de interfaces fueron agregadas en cada slot.

Para realizar el enlace, deberá seguir los siguientes pasos:

1) Hacer clic en el icono  .

2) Hacer clic en el equipo emulado y seleccionar la interface a conectar.

Fig. 3.46 Interfaces disponibles a conectar.

3) Una vez realizada la conexión, hacer clic en el icono  para deshabilitar el proceso de conexión entre equipos emulados.

3.3.5 Enlace con equipo físico.

La herramienta GNS3 también permite conectarse con un equipo físico y permitir ampliar el área de trabajo.

Pasos para conectar un equipo físico a la red virtual:

1) Seleccionar "Cloud" y arrastrarla al área de construcción de topologías.

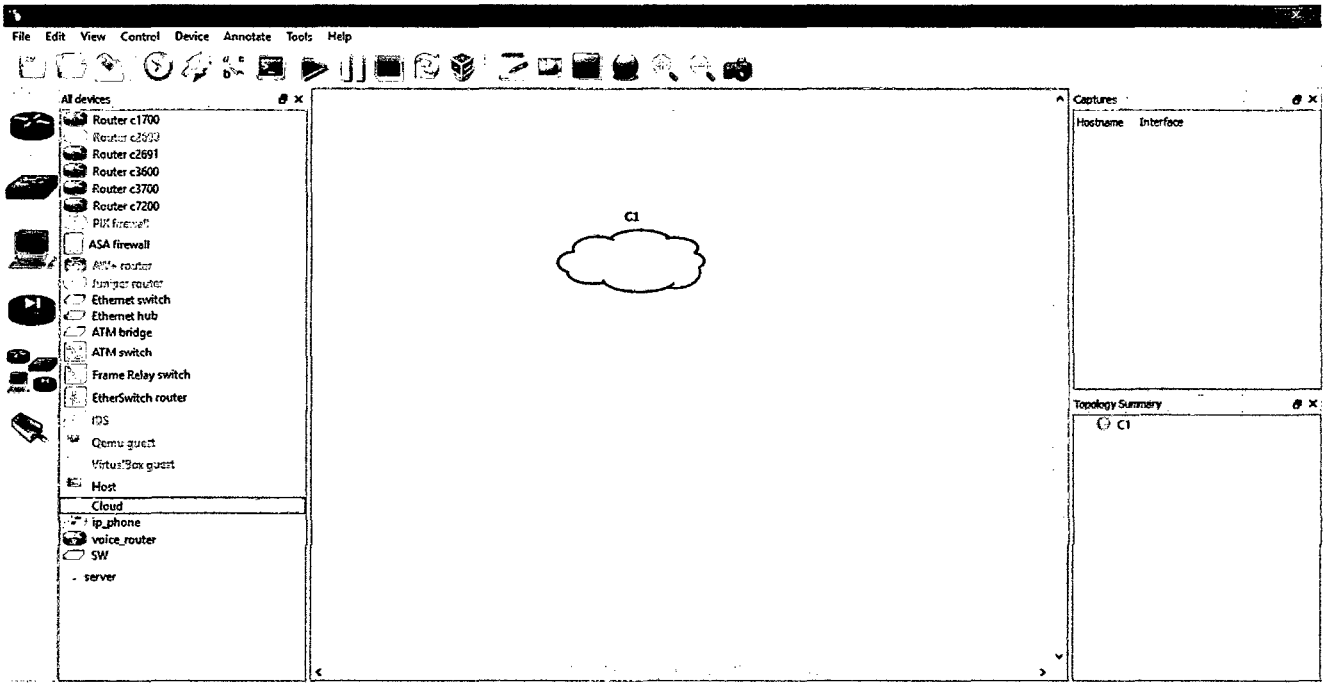


Fig. 3.47 Selección de Cloud.

2) Clic derecho en Cloud y seleccionar "configure".

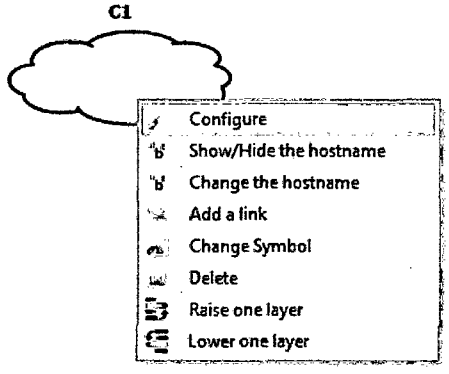


Fig. 3.48 Menú de opciones de Cloud.

3) Clic en "NIO Ethernet" y Luego en "Generic Ethernet NIO" escoger el adaptador de red reconocido por la herramienta GNS3. Seleccionamos la que deseamos utilizar para luego hacer clic en "Apply" y finalmente en "OK".

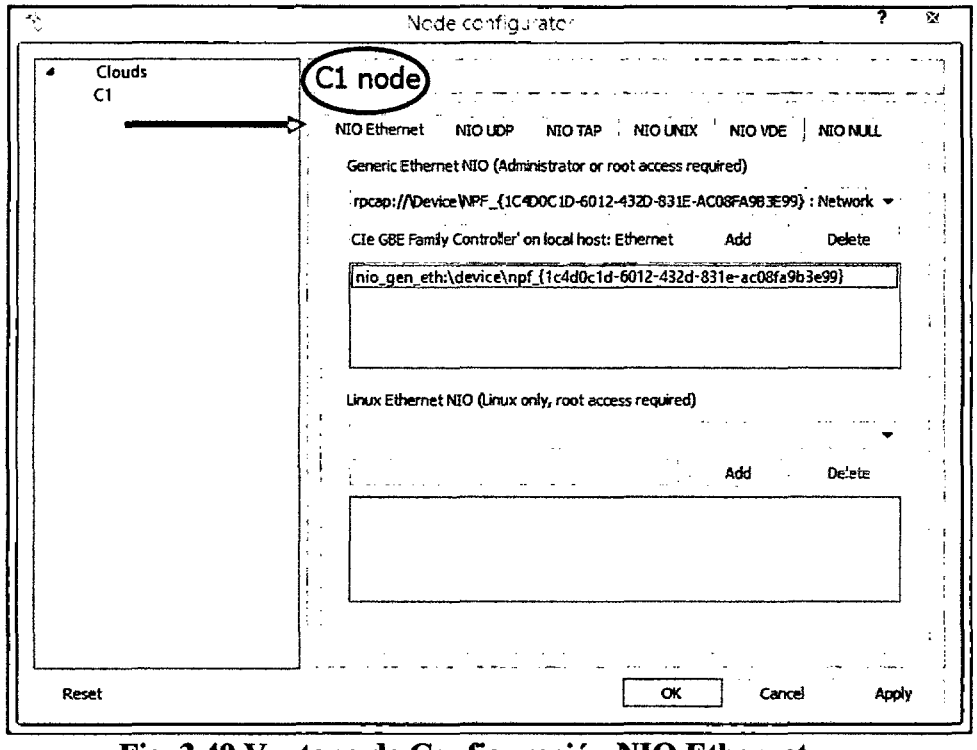


Fig. 3.49 Ventana de Configuración NIO Ethernet.

4) Luego deberá configurar la dirección IP necesaria en el equipo físico para realizar la conexión con el simulador, no olvidar que también configurará la IP en el adaptador de red seleccionado.

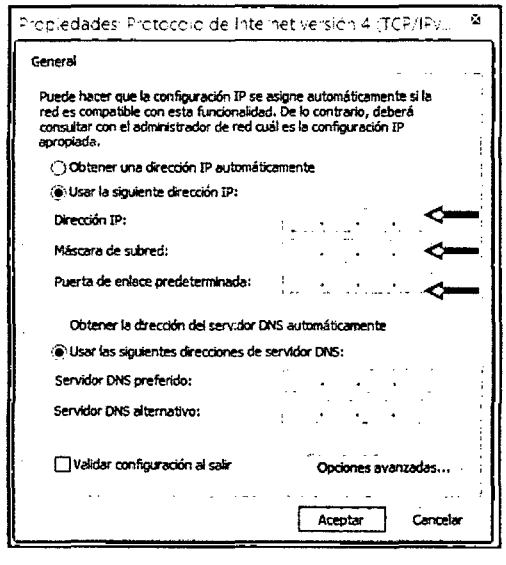


Fig. 3.50 Configuración en Adaptador de red.

5) Finalmente conectar a un router emulado, seleccionando el adaptador de red utilizado.

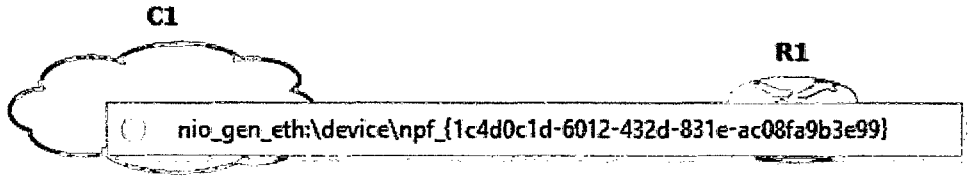


Fig. 3.51 Conexión de Cloud hacia un router emulado.

3.3.6 Captura de datos.

Otra función importante de GNS3 es que puede capturar paquetes, ya sea con el software Wireshark, tcpdump, etc.

Pasos para realizar la captura de paquetes en Wireshark:

1) Hacer clic derecho en la interface que desea capturar paquetes y escoger "Star capturing".

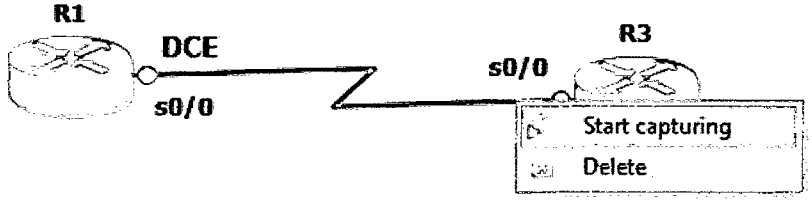


Fig. 3.52 Selección de interface.

2) Luego escoger el tipo de encapsulación que desea utilizar.

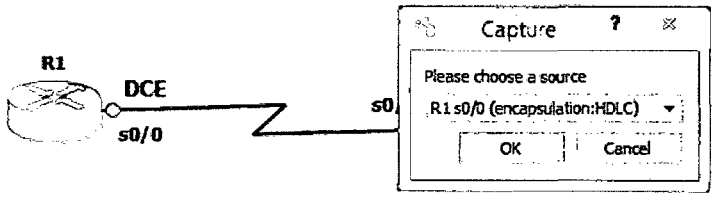


Fig. 3.53 Tipos de encapsulación.

3) Luego clic derecho en el enlace seleccionado y seleccionar "Start Wireshark".

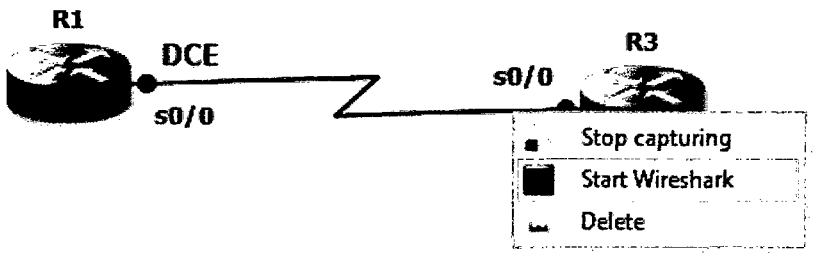


Fig. 3.54 Iniciar captura de paquetes en Wireshark.

4) Finalmente se abrirá Wireshark y se podrá hacer el análisis y estudio de captura de paquetes.

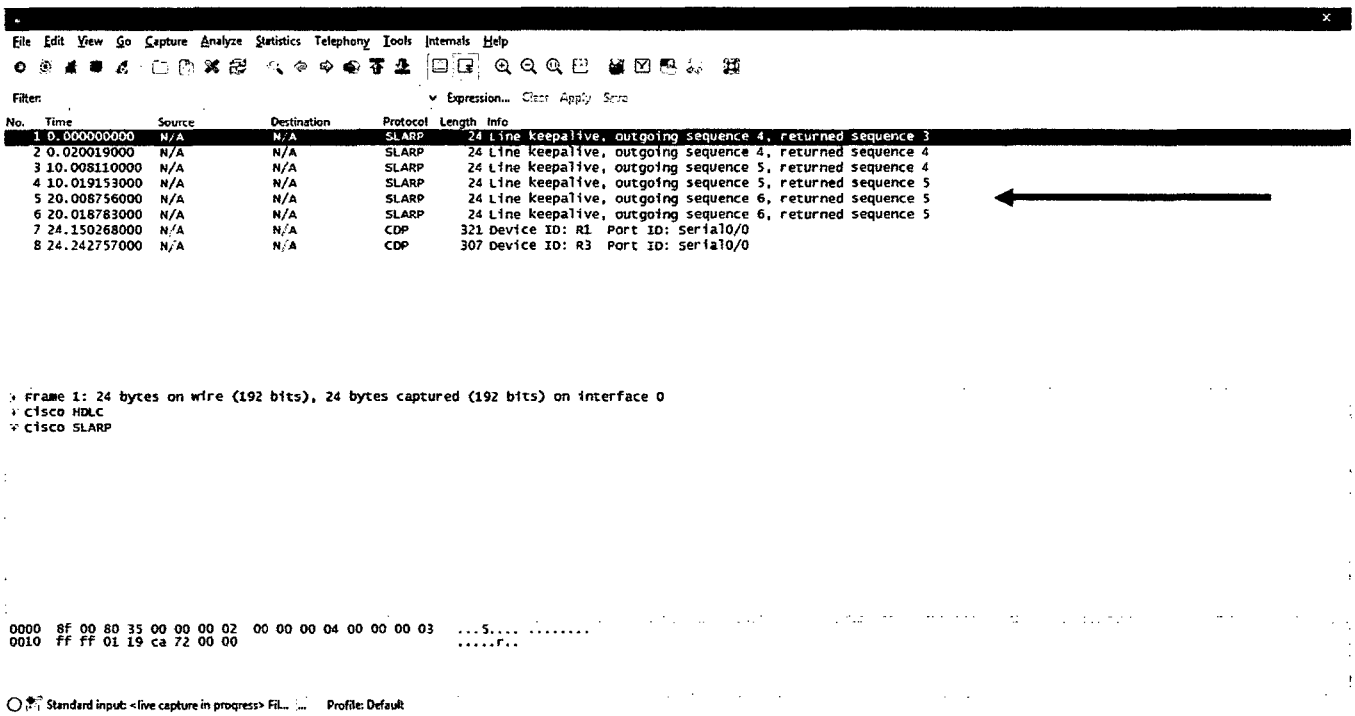


Fig. 3.55 Captura de paquetes en Wireshark.

CAPITULO IV

DISEÑO DE GUIAS DE LABORATORIO CON SIMULADOR GNS3

LABORATORIO 4.1: CONFIGURACION BASICA DE RUTAS ESTATICAS

REVISIÓN TEÓRICA: Para la realización de esta práctica se deberá revisar conceptos de Enrutamiento estático.

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet.
- Configurar una ruta estática por medio de una interfaz de salida.
- Configurar una ruta estática mediante una dirección de siguiente salto.
- Configurar una ruta estática por defecto.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **192.168.10.0/24** para obtener el direccionamiento IP usando VLSM, para los enlaces entre routers y para las diversas LAN, teniendo los siguientes requisitos:

LAN R1: 8 host.
LAN R2: 16 host.
LAN R4: 16 host.

DIAGRAMA DE TOPOLOGIA

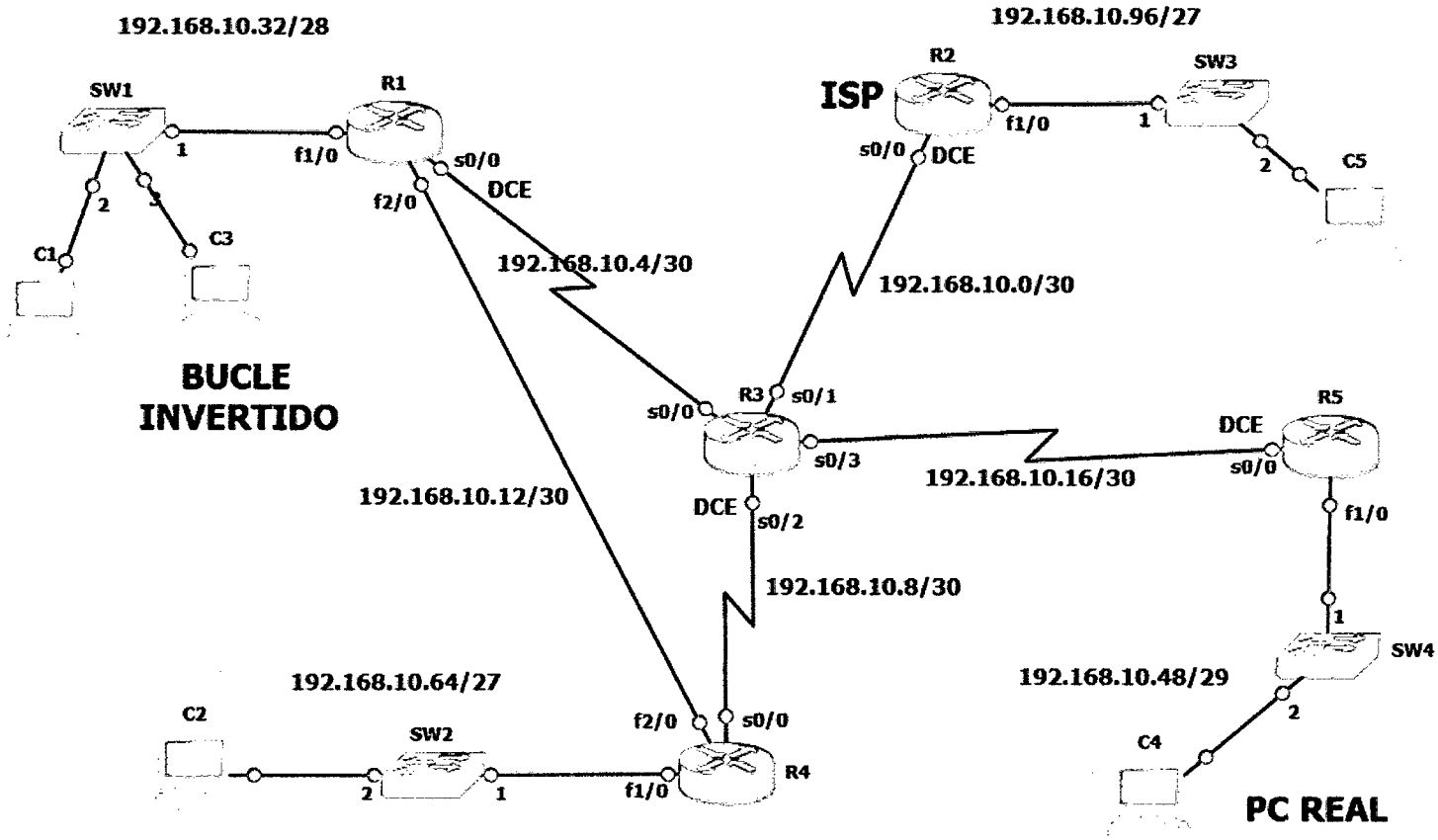


Fig. 4.1.1 Red Virtual en GNS3

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s0/0	192.168.10.6	255.255.255.252	No aplicable
	f1/0	192.168.10.33	255.255.255.240	No aplicable
	f2/0	192.168.10.13	255.255.255.252	No aplicable
R2	s0/0	192.168.10.2	255.255.255.252	No aplicable
	f1/0	192.168.10.97	255.255.255.224	No aplicable
R3	s0/0	192.168.10.5	255.255.255.252	No aplicable
	s0/1	192.168.10.1	255.255.255.252	No aplicable
	s0/2	192.168.10.9	255.255.255.252	No aplicable
	f1/0	192.168.10.17	255.255.255.252	No aplicable
R4	s0/0	192.168.10.10	255.255.255.252	No aplicable
	f1/0	192.168.10.65	255.255.255.224	No aplicable
	f2/0	192.168.10.14	255.255.255.252	No aplicable
R5	s0/0	192.168.10.18	255.255.255.252	No aplicable
	f1/0	192.168.10.49	255.255.255.248	No aplicable
C1	VPCS	192.168.10.34	255.255.255.240	192.168.10.33
C2	VPCS	192.168.10.66	255.255.255.224	192.168.10.65
C3	BUCLE INVERTIDO	192.168.10.35	255.255.255.240	192.168.10.33
C4	NIC	192.168.10.50	255.255.255.248	192.168.10.49
C5	VPCS	192.168.10.98	255.255.255.224	192.168.10.97

Tabla 4.1.1 Direccionamiento IP para las Redes

TAREA 1: MONTAR LA RED EN GNS3

Montar y conectar la red igual a la del Diagrama de topología.

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

Ingrese al modo privilegiado

Router>enable

Aparece el siguiente prompt

Router#

En el modo exec privilegiado, ingrese al modo de configuración global:

Router# **configure terminal**

PASO 1: Establezca la configuración global del nombre de host.

Ingrese el siguiente comando para configurar el nombre del router:

Router(config)#**hostname XXXXXX** (Escribir nombre deseado)

PASO 2: Desactive la búsqueda DNS.

Router(config)# **no ip-domain lookup**

Si escribes algo que no sea un comando de Cisco IOS o cometes un error, el router asume que ha escrito un nombre de dominio y trata de resolver lo que usted escribe, realizando una búsqueda de DNS.

PASO 3: Configure un mensaje para que se muestre al ingresar al router.

Router(config)#**banner motd %** Solo acceso a personal autorizado **%** (Puede escribir cualquier mensaje)

El símbolo % indica el inicio y final del mensaje.

PASO 4: Configure las contraseñas de consola, enable secret y VTY.

Seguir los siguientes pasos:

Router(config)# **line console 0**

Router(config-line)# **password XXXXX** (Escribir contraseña deseada)

Router(config-line)# **login**

Router(config-line)# **exit**

Router(config)# **enable secret XXXXX** (Escribir contraseña deseada)

Router(config)# **line vty 0 4**

Router(config-line)# **password XXXXX** (Escribir contraseña deseada)

Router(config-line)# **login**

Router(config-line)# **exit**

PASO 5: Sincronice los mensajes no solicitados y el resultado de la depuración con el resultado solicitado y los indicadores para las líneas de consola y de terminal virtual.

Router(config)# **line console 0**

Router(config)# **logging synchronous**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **logging synchronous**

Router(config)# **exit**

PASO 6: Configure un tiempo de espera EXEC de 10 minutos.

Router(config)# **line console 0**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

PASO 7: Guardar la configuración.

Router(config)# **copy running-config startup-config**

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET.

R1:

Configuración para una interface serial:

R1(config)# **interface serial 0/0**

R1(config-if)# **description conexion a R3**

R1(config-if)# **ip address 192.168.10.6 255.255.255.252**

R1(config-if)# **clock rate 64000**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

Configuración para una interface fasEthernet:

R1(config)# **interface fasEthernet 1/0**

R1(config-if)# **description conexion a LAN R1**

R1(config-if)# **ip address 192.168.10.33 255.255.255.224**

R1(config-if)# **no shutdown**

R1(config-if)# **end**

NOTA: Seguir los mismos pasos para las demás routers.

TAREA 4: CONFIGURAR LAS RUTAS ESTÁTICAS MEDIANTE UNA DIRECCIÓN DE SIGUIENTE SALTO, POR MEDIO DE UNA INTERFAZ DE SALIDA O POR DEFECTO.

PASO 1: Para configurar rutas estáticas con un siguiente salto específico, utilice la siguiente sintaxis:

Router(config)# **ip route** [network-address] [subnet-mask] [ip-address]

- **network-address:** dirección de destino de la red remota que se deberá agregar en la tabla de enrutamiento.
- **subnet-mask:** máscara de subred de la red remota que se deberá agregar en la tabla de enrutamiento. La máscara de subred puede modificarse para resumir un grupo de redes.
- **ip-address:** generalmente denominada dirección IP del router de siguiente salto.

R1:

R1#**configure terminal**

R1(config)#**ip route 192.168.10.0 255.255.255.252 s0/0**

R1(config)#**ip route 192.168.10.8 255.255.255.252 s0/0**

R1(config)# **ip route 192.168.10.16 255.255.255.252 s0/0**

R1(config)# **ip route 192.168.10.48 255.255.255.248 s0/0**

R1(config-if)#**exit**

PASO 2: Para configurar rutas estáticas con una interfaz de salida específica, utilice la siguiente sintaxis:

Router(config)# **ip route** [network-address] [subnet-mask] [exit-interface]

- **network-address:** dirección de destino de la red remota que se deberá agregar en la tabla de enrutamiento.
- **subnet-mask:** máscara de subred de la red remota que se deberá agregar en la tabla de enrutamiento. La máscara de subred puede modificarse para resumir un grupo de redes.
- **exit-interface:** interfaz de salida que se utilizaría para reenviar paquetes a la red de destino.

R1:

R1#**configure terminal**

R1(config)#**ip route 192.168.10.64 255.255.255.224 192.168.10.14**

R1(config-if)#**exit**

NOTA: *Seguir los mismos pasos para los demás routers.*

PASO 3: Para configurar rutas estáticas por defecto, utilice la siguiente sintaxis:

Una ruta estática por defecto es similar a cualquier otra ruta estática, excepto que la dirección de red es 0.0.0.0 y la máscara de subred es 0.0.0.0:

Router(config)#ip route 0.0.0.0 0.0.0.0 [exit-interface | ip-address]

- **exit-interface:** interfaz de salida que se utilizaría para reenviar paquetes a la red de destino.
- **ip-address:** generalmente denominada dirección IP del router de siguiente salto.

R1:

R1#**configure terminal**

R1(config)#**ip route 0.0.0.0 0.0.0.0 s0/0**

R1(config-if)#**exit**

TAREA 5: CONFIGURAR LOS EQUIPOS DE HOST.

VPCS

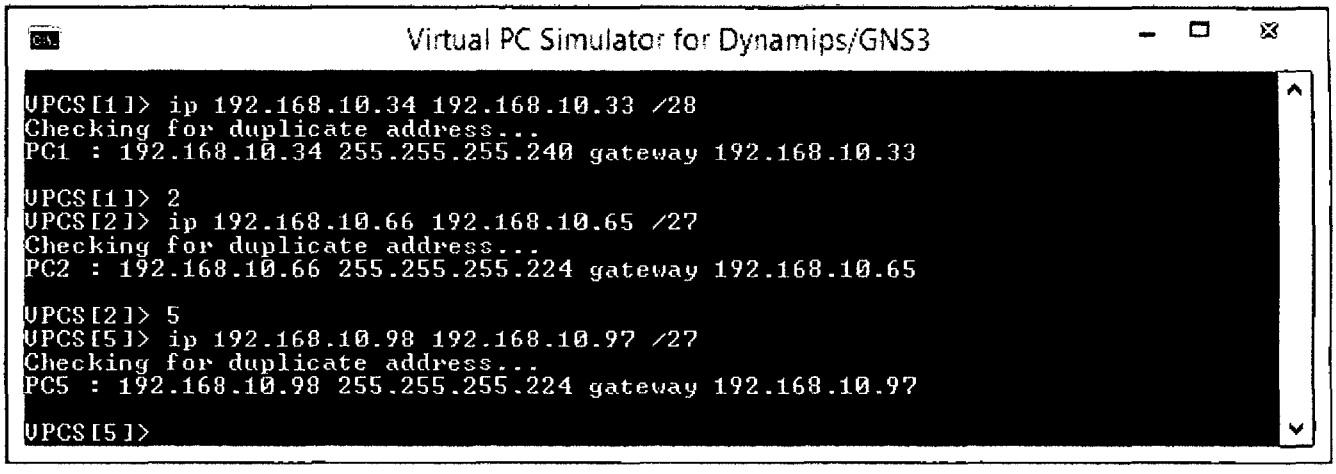


Fig. 4.1.2 Configuración de IP para VPCS.

PC REAL

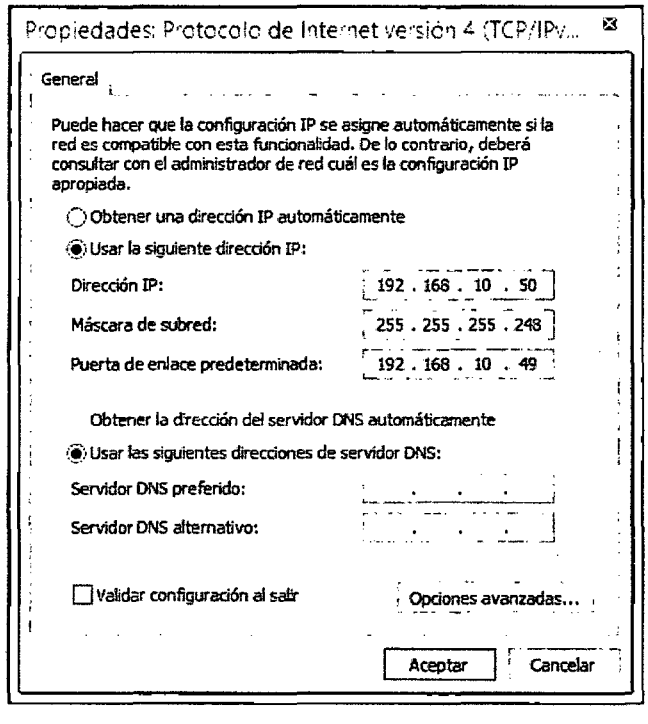


Fig. 4.1.3 Configuración de IP para PC REAL.

NOTA: Configurar los demás host.

TAREA 6: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

PASO 1: Verificar configuraciones.

R3#show ip route

Muestra el contenido de la tabla de enrutamiento IP.

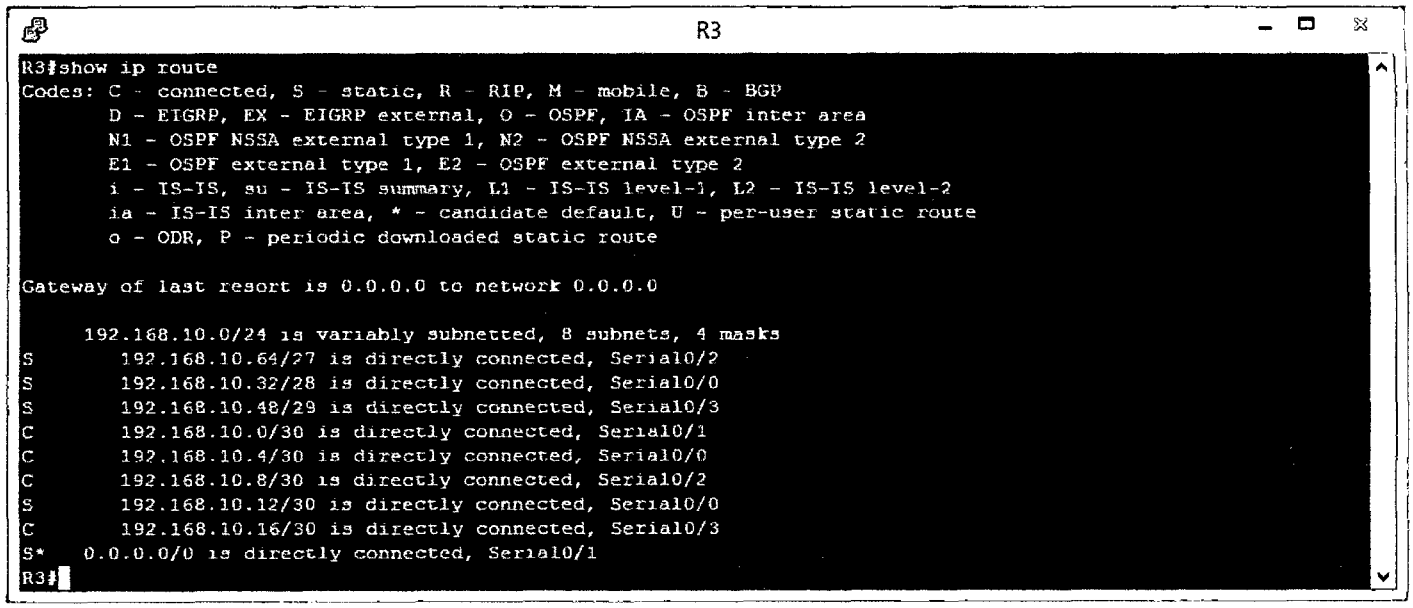


Fig. 4.1.4 Tabla de enrutamiento de R3.

R3#show ip interface brief

Muestra un breve resumen de la información y del estado de una dirección IP.

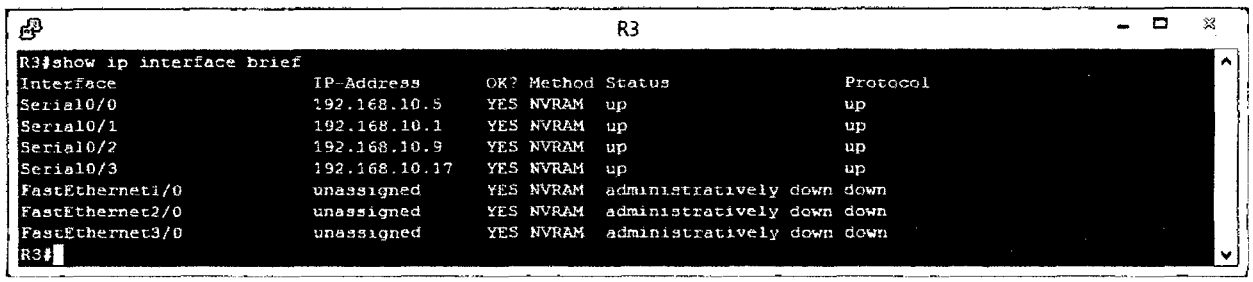


Fig. 4.1.5 Tabla ip interface brief.

R3#**show running-config**

Muestra la configuración actual en la RAM.

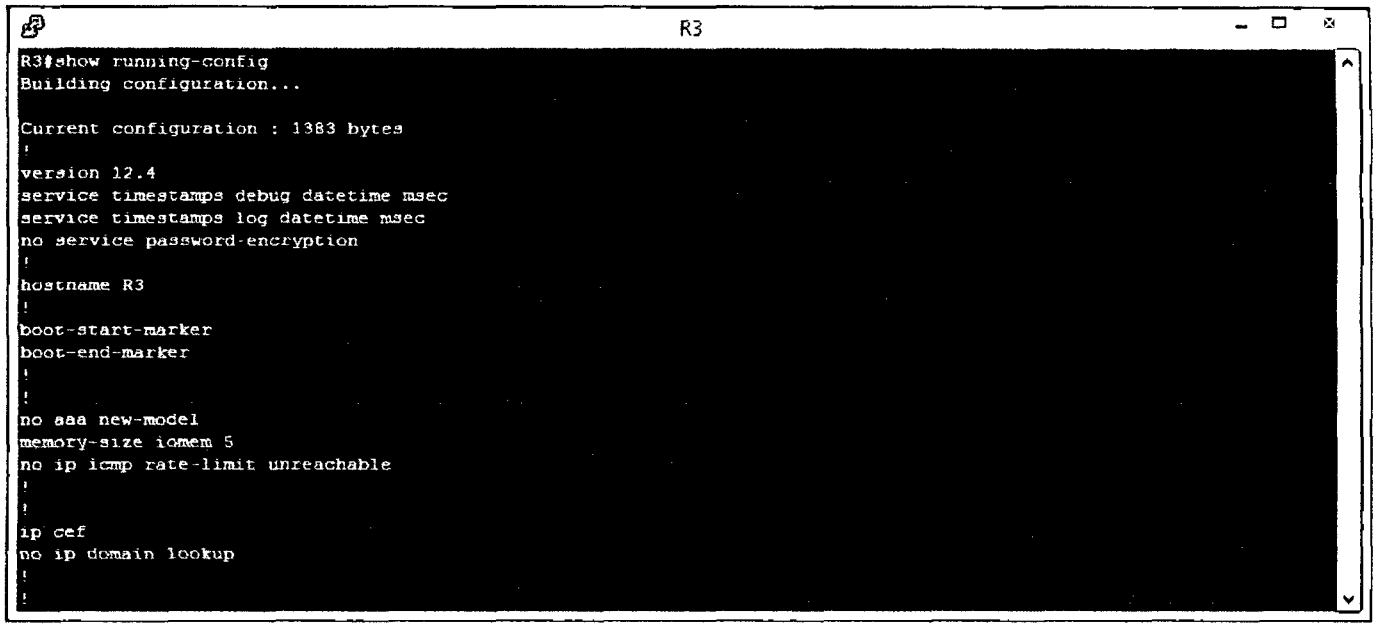


Fig. 4.1.6 Show running-config de R3.

R3#**show cdp neighbors**

Muestra información detallada de todos los dispositivos Cisco que están conectados localmente.

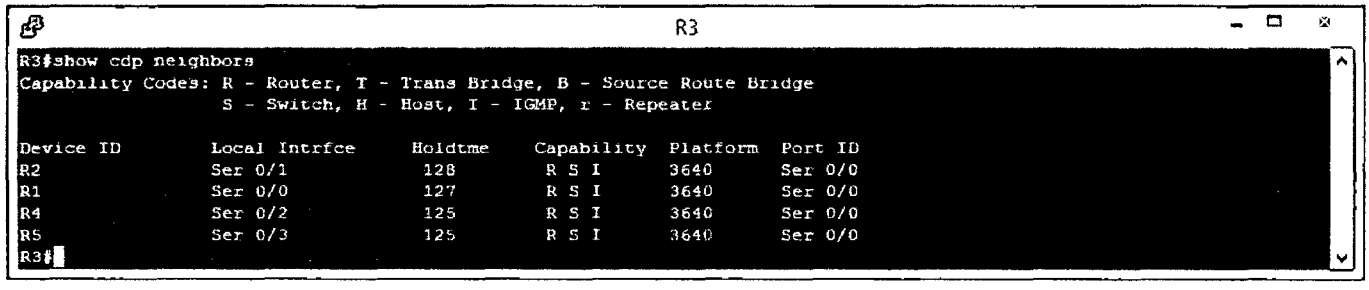


Fig. 4.1.7 Tabla cdp neighbors.

NOTA: Realizar estos comandos para los demás routers, verificando así cualquier error.

PASO 2: Utilice el comando ping para probar la conectividad entre los routers que *no están directamente conectados y también la conectividad entre host.*

PING ENTRE ROUTERS

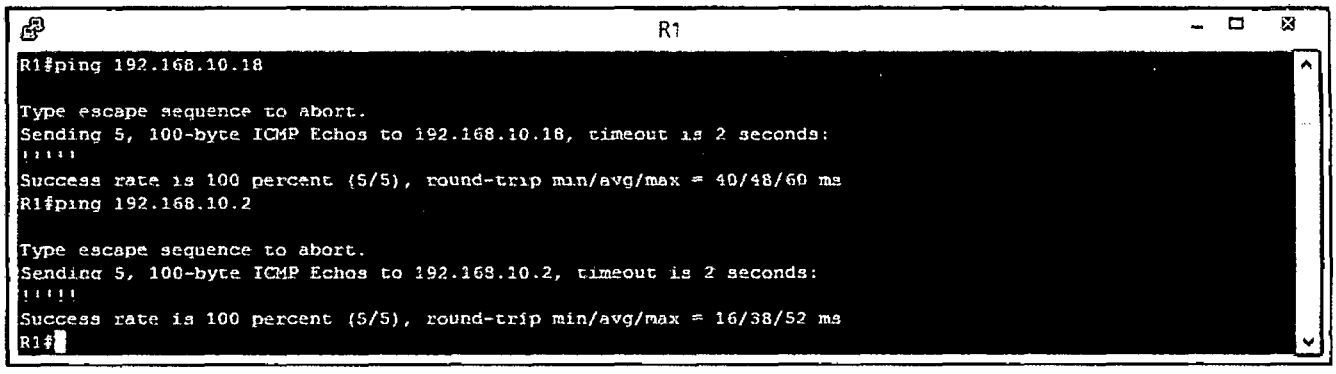


Fig. 4.1.8 Prueba de conectividad entre routers.

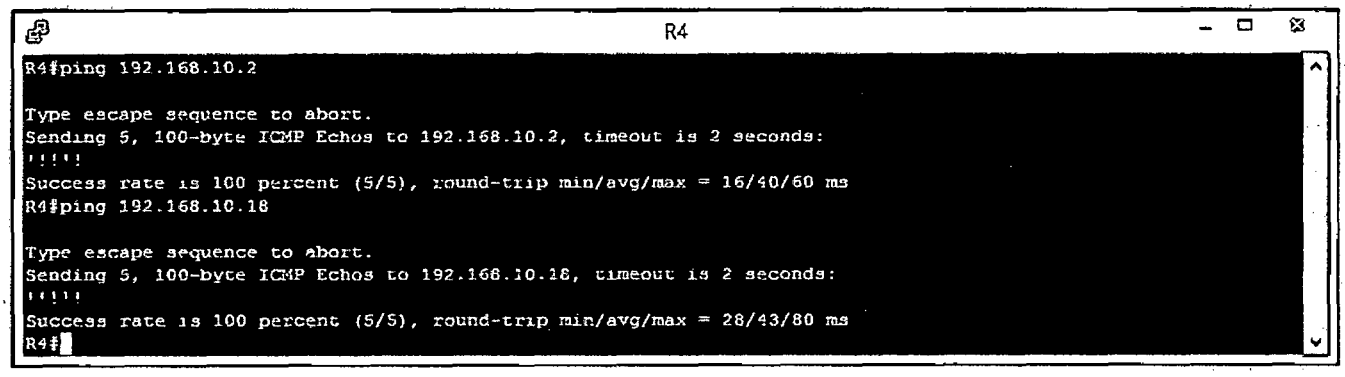


Fig. 4.1.9 Prueba de conectividad entre routers.

PING ENTRE HOST

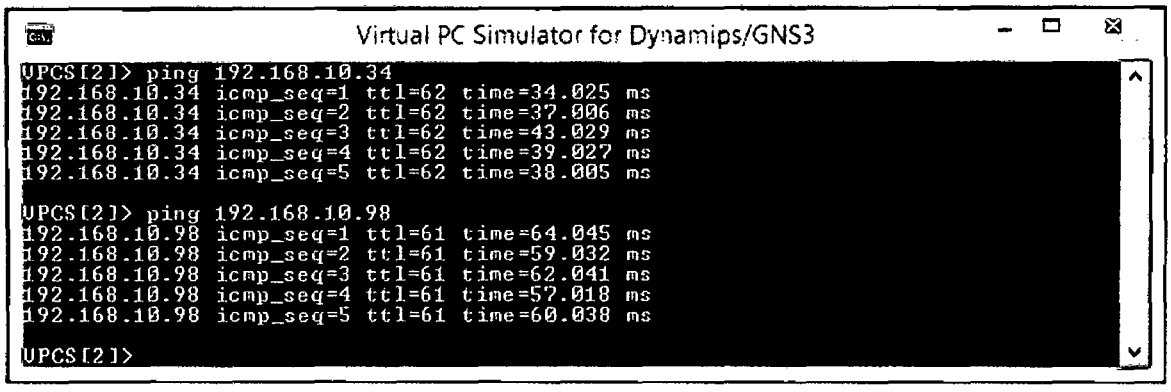


Fig. 4.1.10 Prueba de conectividad entre host.

NOTA: Realizar las pruebas faltantes.

TAREA 7: ANALISIS DEL TRAFICO DE PAQUETES

PASO 1: Medición de la Latencia

Para la medición de la latencia se realizó 10 muestras sucesivas de 100 ping desde el C3 (Bucle invertido) hacia la PC REAL considerando un tamaño de trama de 64, 512 y 1518 bytes como se especifica en el RFC 2544.

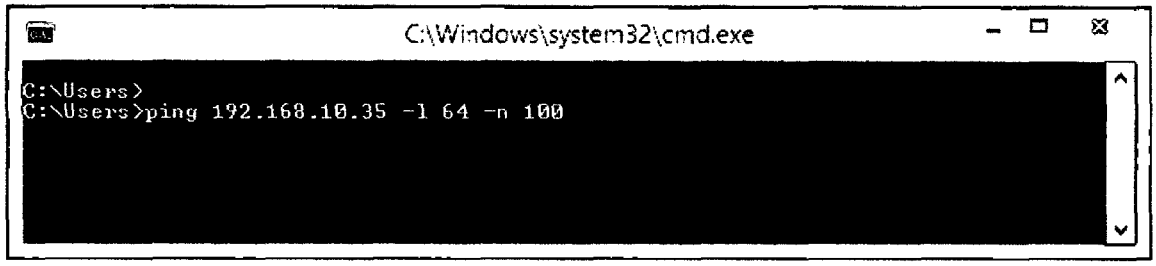


Fig. 4.1.11 Forma de medición de la latencia.

En la Figura 4.1.11 se puede observar el envío de 100 ping con una trama de 64 hacia la dirección 192.168.10.35

En las Tablas posteriores se detallan los valores de la Latencia que se ha obtenido una vez realizadas todas las muestras.

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	N° 1	**N° 2**	**N° 3**	**N° 4**	**N° 5**	**N° 6**	**N° 7**	**N° 8**	**N° 9**	**N° 10**	**Promedio**
Tiempo Mínimo (ms)	**82**	**79**	**80**	**79**	**79**	**84**	**84**	**79**	**84**	**80**	**81**
Tiempo Máximo (ms)	**93**	**97**	**92**	**97**	**94**	**93**	**95**	**95**	**92**	**99**	**94.7**
Tiempo Promedio (ms)	**87**	**87**	**85**	**85**	**85**	**89**	**88**	**85**	**88**	**85**	**86.4**

Tabla 4.1.2 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	512										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	80	75	80	81	87	88	74	78	79	82	80.4
Tiempo Máximo (ms)	94	95	95	96	94	98	92	99	98	91	95.2
Tiempo Promedio (ms)	89	90	91	84	90	90	88	89	90	87	88.8

Tabla 4.1.3 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1518										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	111	112	112	108	119	111	115	110	109	110	111.7
Tiempo Máximo (ms)	120	124	121	127	123	127	131	141	126	126	126.6
Tiempo Promedio (ms)	115	119	117	117	121	117	119	119	117	117	117.8

Tabla 4.1.4 Datos obtenidos para una trama de 1518 bytes.

LATENCIA			
Tamaño de Trama (bytes)	64	512	1518
Tiempo Mínimo (ms)	81	80.4	111.7
Tiempo Máximo (ms)	94.7	95.2	126.6
Tiempo Promedio (ms)	86.4	88.8	117.8

Tabla 4.1.5 Comparación de datos obtenidos de las diferentes tramas.

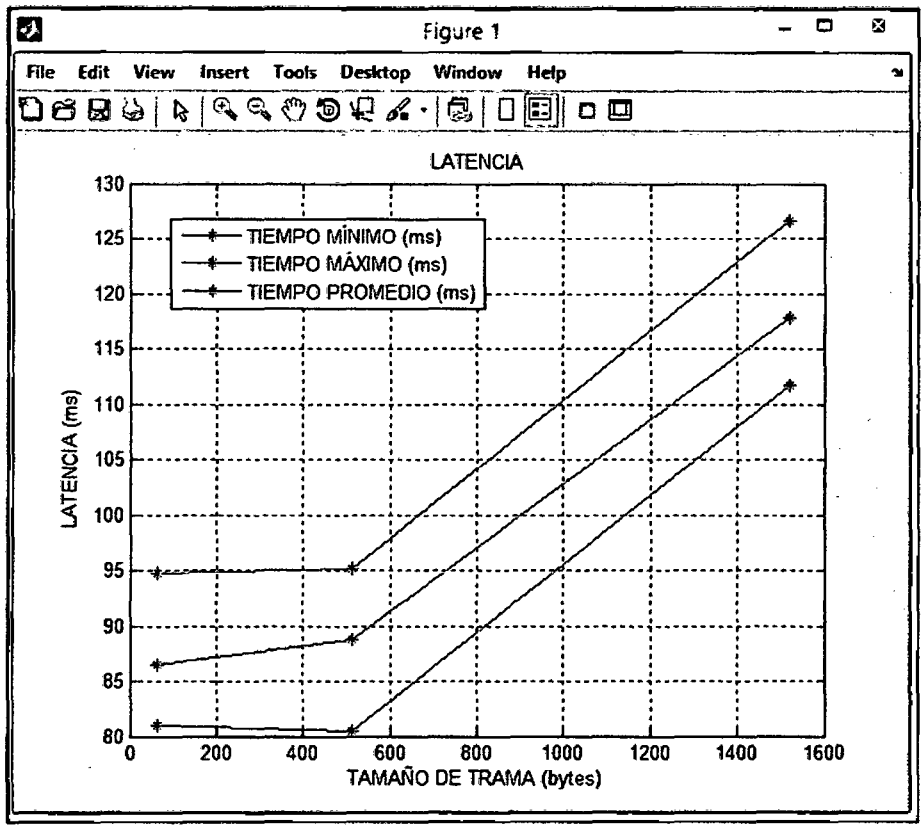


Fig. 4.1.12 Datos representados gráficamente de la variación de la latencia.

De acuerdo con los datos obtenidos, se puede observar claramente que los valores mínimo (color azul), máximo (color rojo) y promedio (color verde) de la latencia de la red se incrementan conforme se envía una trama de longitud mayor, en este caso con la trama de 1518 bytes se obtiene una latencia promedio de 117.8 ms a diferencia de una trama de 64 bytes con 86.4 ms.

PASO 2: Medición del Throughput

Para la medición del Throughput y Jitter se envió una cantidad de tramas a velocidades diferentes durante 20 segundos, hasta encontrar la máxima cantidad de tramas recibidas sin que se produzcan perdidas de las mismas en el router y PC REAL. Como se utilizó Jperf el cliente será el encargado de enviar los paquetes y el servidor los recibirá, indicando la cantidad de paquetes que llegaron correctamente considerando un tamaño del paquete UDP de 750, 1125, 1500 y 1470 (default) bytes, tal como se especifica en el RFC 768.

Configuración del Jperf como servidor con UDP Packet Size de 1500 Bytes.

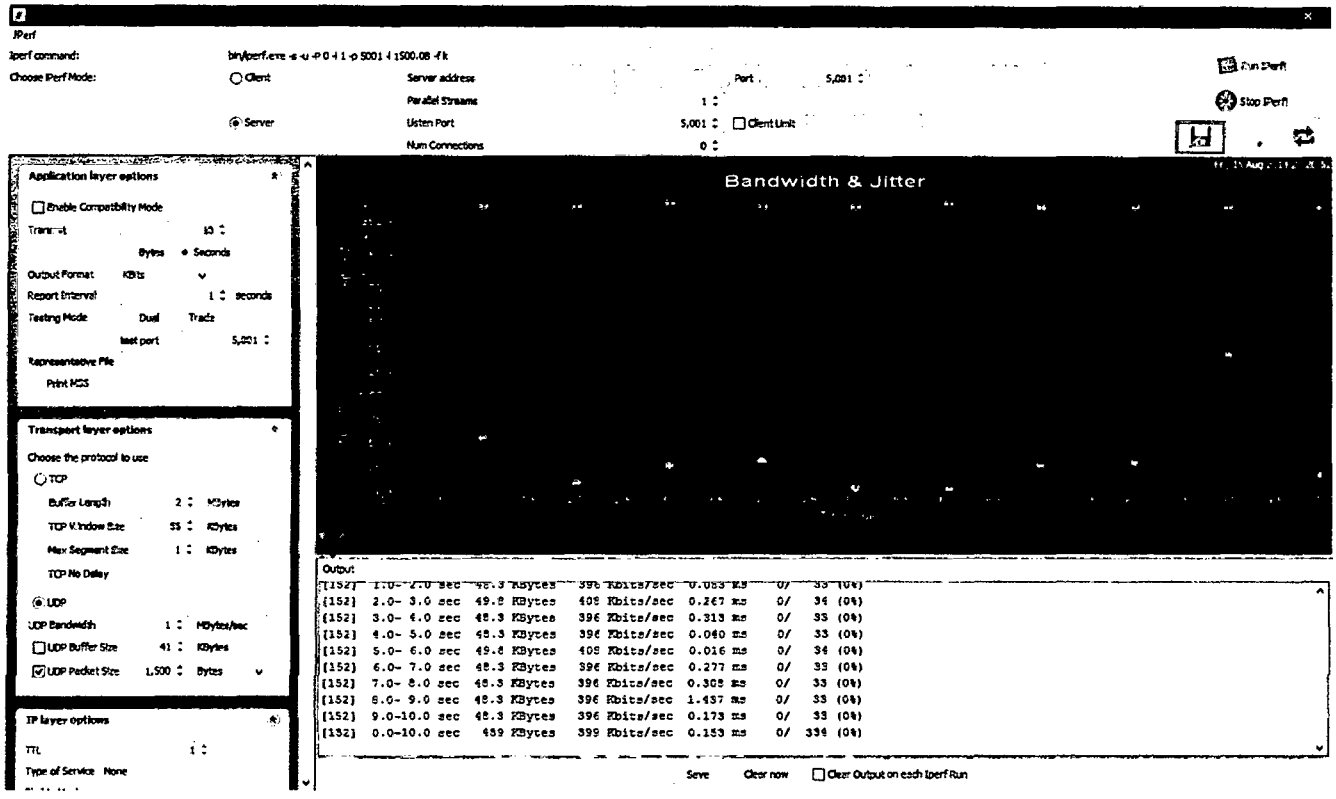


Fig. 4.1.13 Gráfica de Bandwidth y Jitter.

```
bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -l 1500.0B -f k
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1500 byte datagrams
UDP buffer size: 64.0 KByte (default)
------------------------------------------------------------
OpenSCManager failed - Acceso denegado. (0x5)
[152] local 192.168.10.50 port 5001 connected with 192.168.10.35 port 58613
[ ID] Interval       Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[152]  0.0- 1.0 sec  48.3 KBytes   396 Kbits/sec  0.557 ms 1546661425/   33 (4.7e+009%)
[152]  1.0- 2.0 sec  48.3 KBytes   396 Kbits/sec  0.083 ms    0/   33 (0%)
[152]  2.0- 3.0 sec  49.8 KBytes   408 Kbits/sec  0.267 ms    0/   34 (0%)
[152]  3.0- 4.0 sec  48.3 KBytes   396 Kbits/sec  0.313 ms    0/   33 (0%)
[152]  4.0- 5.0 sec  48.3 KBytes   396 Kbits/sec  0.040 ms    0/   33 (0%)
[152]  5.0- 6.0 sec  49.8 KBytes   408 Kbits/sec  0.016 ms    0/   34 (0%)
[152]  6.0- 7.0 sec  48.3 KBytes   396 Kbits/sec  0.277 ms    0/   33 (0%)
[152]  7.0- 8.0 sec  48.3 KBytes   396 Kbits/sec  0.308 ms    0/   33 (0%)
[152]  8.0- 9.0 sec  48.3 KBytes   396 Kbits/sec  1.437 ms    0/   33 (0%)
[152]  9.0-10.0 sec  48.3 KBytes   396 Kbits/sec  0.173 ms    0/   33 (0%)
[152]  0.0-10.0 sec   489 KBytes   399 Kbits/sec  0.153 ms    0/  334 (0%)
```

Fig. 4.1.14 Resultados al medir como servidor.

Configuración del Jperf como cliente con UDP Bandwidth de 400 Kb y UDP Packet Size de 1500 Bytes.

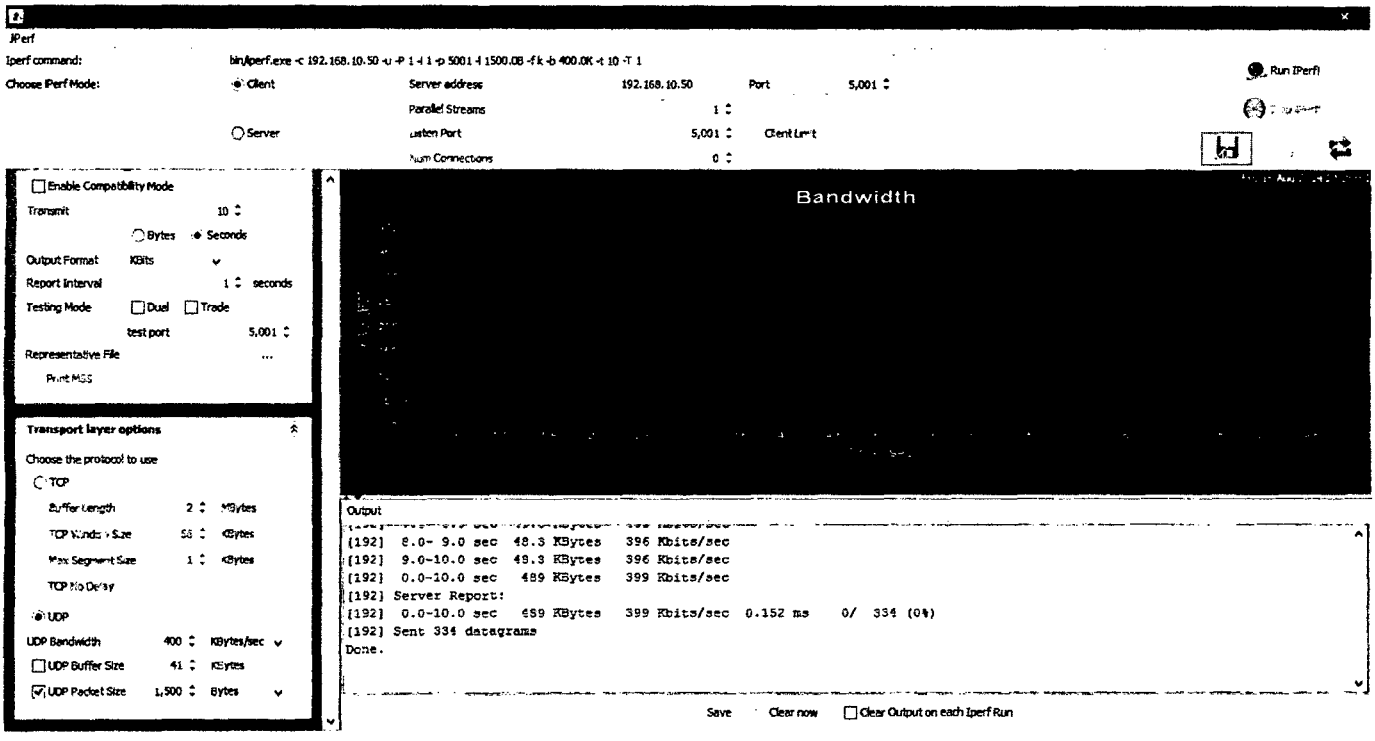


Fig. 4.1.15 Resultados del Jperf como Cliente.

En las siguientes Tablas se detalla los valores del Throughput obtenidos una vez realizada todas las muestras.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**0.4**	**0.4**	**0.4**
Velocidad de Rx (Mbps)	**0.4**	**0.4**	**0.4**
Tramas Transmitidas	**667**	**445**	**334**
Tramas Recibidas	**667**	**445**	**334**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**66.7**	**44.5**	**33.4**

Tabla 4.1.6 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**0.4**	**0.5**	**0.8**
Velocidad de Rx (Mbps)	**0.4**	**0.5**	**0.8**
Tramas Transmitidas	**341**	**426**	**681**
Tramas Recibidas	**341**	**426**	**681**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**34.1**	**42.6**	**68.1**

Tabla 4.1.7 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

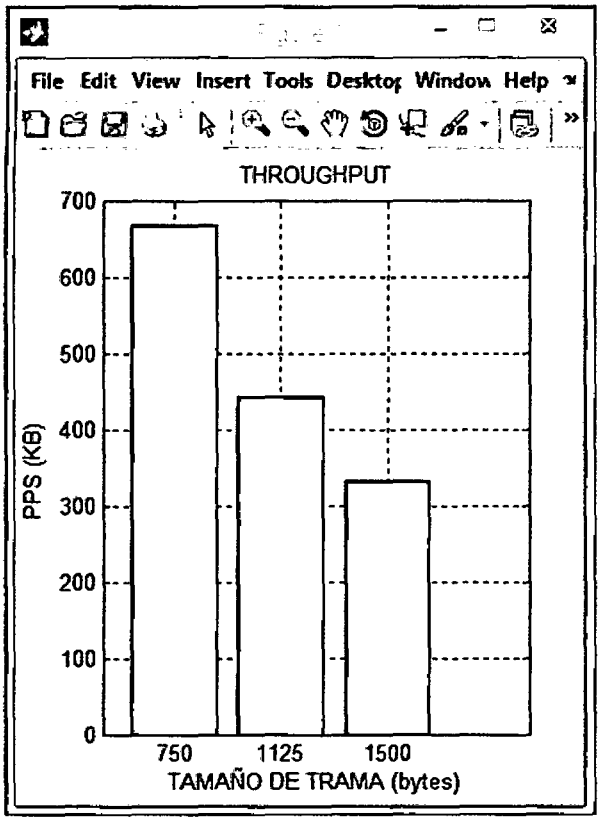


Fig. 4.1.16 PPS vs. Tamaño de Trama.

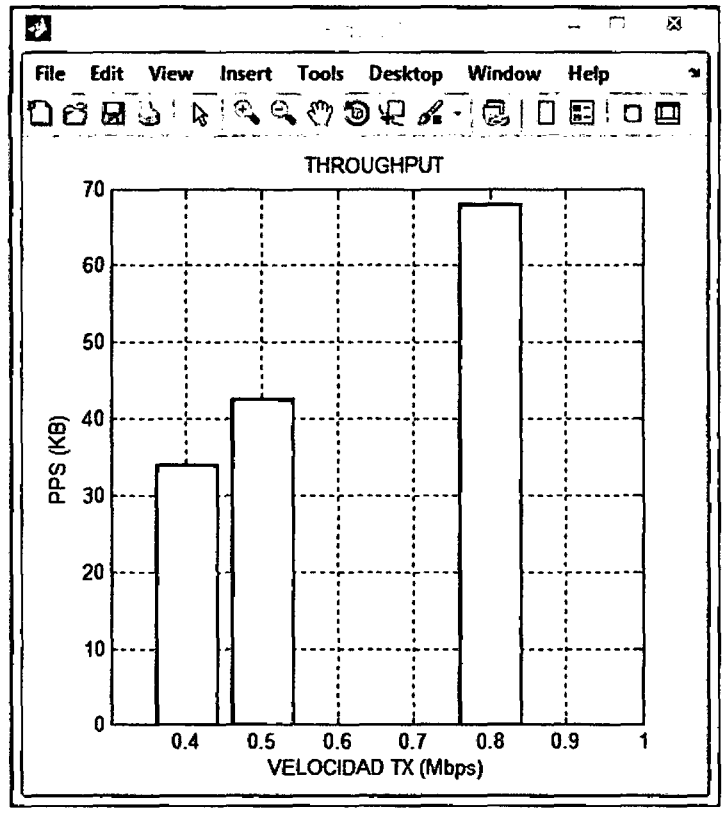


Fig. 4.1.17 PPS vs. Velocidad Tx.

En la figura 4.1.16, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 750 bytes, 1125 bytes y 1500 bytes los cuales han utilizado una velocidad de Tx constante de 0.4 Mbps, en la gráfica se puede observar claramente que al enviar una trama de 750 bytes se envía 667 pps, con una trama de 1125 se envía 445 pps y con una trama de 1500 se envía 334 pps.

Mientras en la figura 4.1.17, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 1470 bytes los cuales han utilizado una velocidad de Tx variada de: 0.4 Mbps, 0.5 Mbps y 0.8 Mbps, sin que se produzcan perdidas en el envío, como los datos que se muestran en la tabla 4.1.7.

PASO 3: Medición del Jitter

Para la medición se envió datos UDP de longitud variable a velocidades diferentes de Throughput obtenida anteriormente durante 20 segundos. Como se utilizó anteriormente Jperf el cliente será el encargado de enviar los datos y el servidor los recibirá, indicando los valores de Jitter obtenidos durante la transmisión de los datos.

En las siguientes Tablas se detalla los valores del Jitter obtenidos una vez realizada todas las muestras.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**0.4**	**0.4**	**0.4**
Velocidad de Rx (Mbps)	**0.4**	**0.4**	**0.4**
Tramas Transmitidas	**667**	**445**	**334**
Tramas Recibidas	**667**	**445**	**334**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**0.050**	**0.096**	**0.153**

Tabla 4.1.8 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**0.4**	**0.5**	**0.8**
Velocidad de Rx (Mbps)	**0.4**	**0.5**	**0.8**
Tramas Transmitidas	**341**	**426**	**681**
Tramas Recibidas	**341**	**426**	**681**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**0.146**	**0.247**	**0.312**

Tabla 4.1.9 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

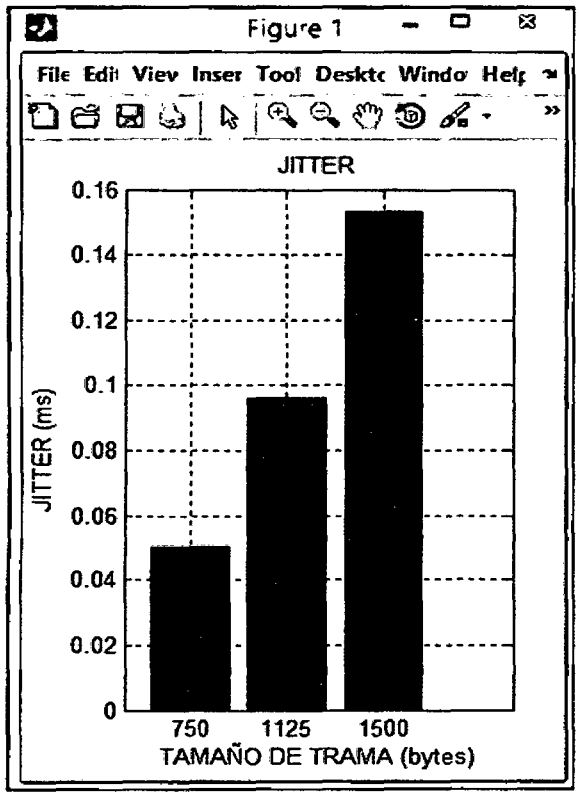


Fig. 4.1.18 Jitter vs. Tamaño de Trama

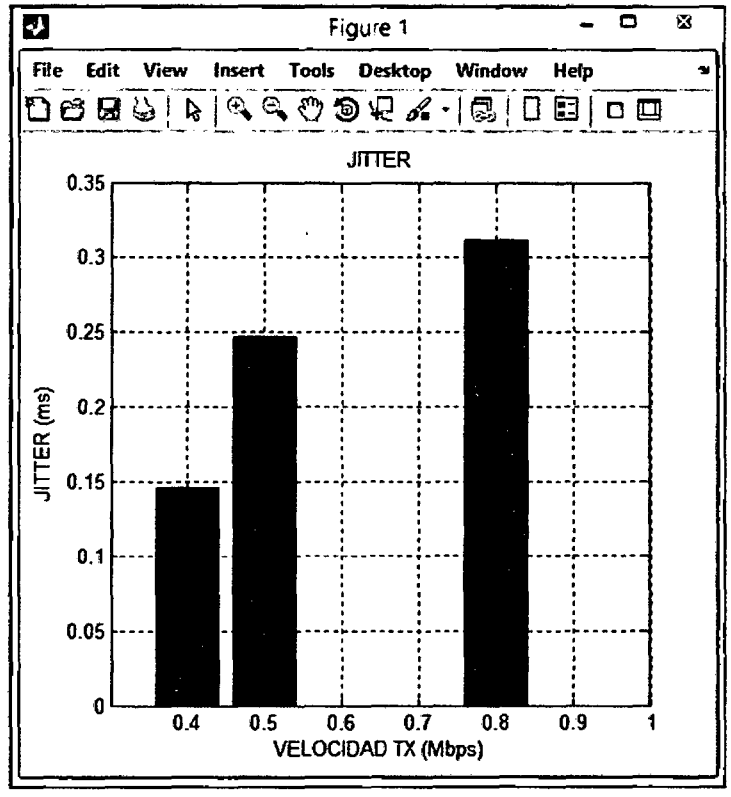


Fig. 4.1.19 Jitter vs. Velocidad Tx

En la figura 4.1.18 se observa los valores del Jitter obtenidos al enviar diferentes tamaños de paquete UDP como 750, 1125 y 1500 bytes utilizando una velocidad de Tx constante de 0.4 Mbps, se puede observar claramente que con una trama de 750 bytes se tiene un Jitter de 0.050 ms a diferencia de la trama de 1500 bytes en la cual se tiene un Jitter de 0.153 ms.

En la figura 4.1.19, se observa los valores del Jitter obtenidos al enviar paquetes UDP de 1470 bytes utilizando una velocidad de Tx que varía entre 0.4 Mbps, 0.5 Mbps y 0.8 Mbps sin que se pierdan paquetes en la red, concluyendo también que a mayor ancho de banda mucho mayor será el jitter y habrá pérdidas de datagramas.

Configuración del Jperf como cliente con UDP Bandwidth de 1 Mbps y UDP Packet Size por defecto.

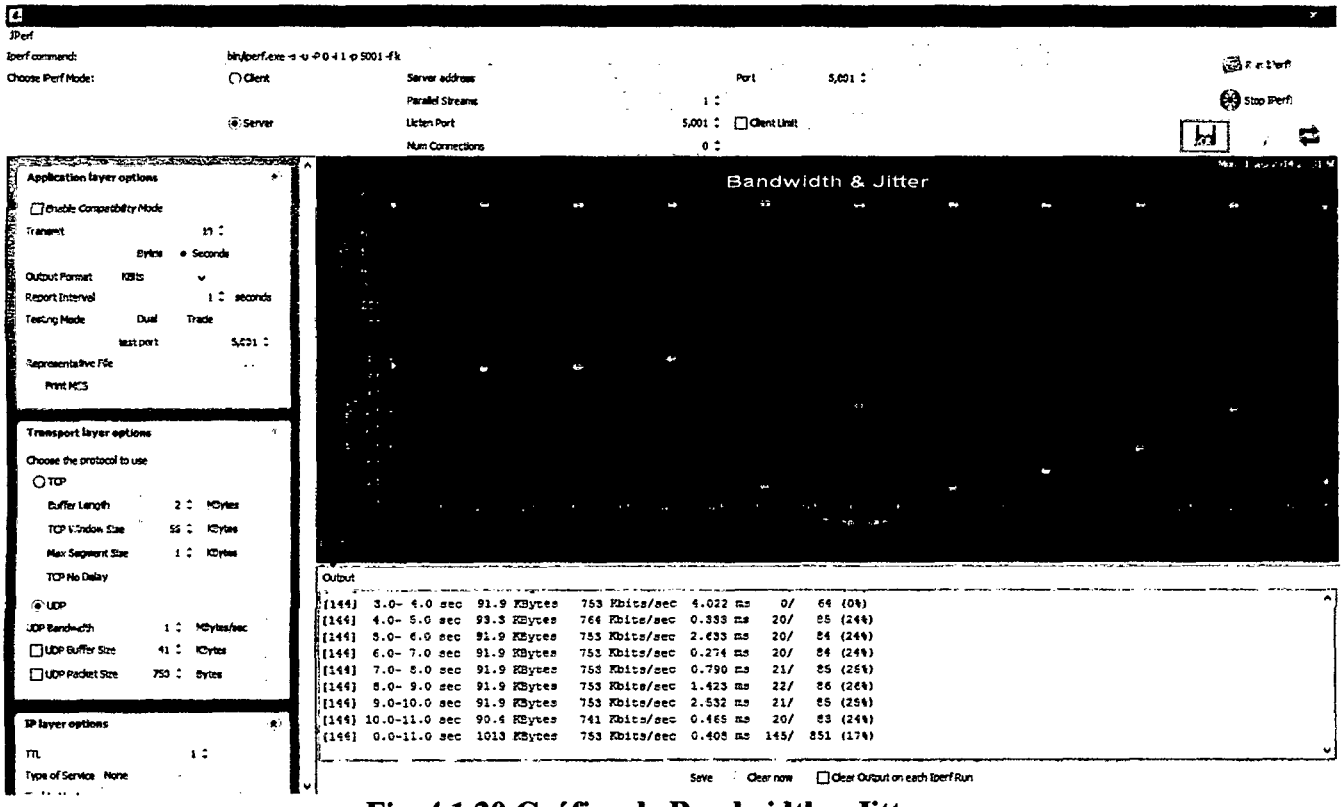


Fig. 4.1.20 Gráfica de Bandwidth y Jitter.

Se observa un aumento de Jitter y por consecuencia hay pérdidas de datagramas.

```
bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -f k
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 64.0 KByte (default)
------------------------------------------------------------
OpenSCManager failed - Acceso denegado. (0x5)
[144] local 192.168.10.50 port 5001 connected with 192.168.10.35 port 57695
[ ID] Interval       Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[144]  0.0- 1.0 sec  91.9 KBytes   753 Kbits/sec  3.817 ms 1415071048/   64 (2.2e+009%)
[144]  1.0- 2.0 sec  91.9 KBytes   753 Kbits/sec  3.728 ms    0/   64 (0%)
[144]  2.0- 3.0 sec  91.9 KBytes   753 Kbits/sec  3.773 ms    0/   64 (0%)
[144]  3.0- 4.0 sec  91.9 KBytes   753 Kbits/sec  4.022 ms    0/   64 (0%)
[144]  4.0- 5.0 sec  93.3 KBytes   764 Kbits/sec  0.333 ms   20/   85 (24%)
[144]  5.0- 6.0 sec  91.9 KBytes   753 Kbits/sec  2.633 ms   20/   84 (24%)
[144]  6.0- 7.0 sec  91.9 KBytes   753 Kbits/sec  0.274 ms   20/   84 (24%)
[144]  7.0- 8.0 sec  91.9 KBytes   753 Kbits/sec  0.790 ms   21/   85 (25%)
[144]  8.0- 9.0 sec  91.9 KBytes   753 Kbits/sec  1.423 ms   22/   86 (26%)
[144]  9.0-10.0 sec  91.9 KBytes   753 Kbits/sec  2.532 ms   21/   85 (25%)
[144] 10.0-11.0 sec  90.4 KBytes   741 Kbits/sec  0.465 ms   20/   83 (24%)
[144]  0.0-11.0 sec  1013 KBytes   753 Kbits/sec  0.408 ms  145/  851 (17%)
```

Fig. 4.1.21 Resultados al medir como servidor.

PASO 4: Captura de tráfico con Wireshark.

Capturar tráfico de paquetes en la interfaz s0/0 de R5.

- Captura de paquetes SLARP (Serial Line Address Resolution Protocol), se utiliza en líneas seriales para asignar una dirección IP a una interfaz.

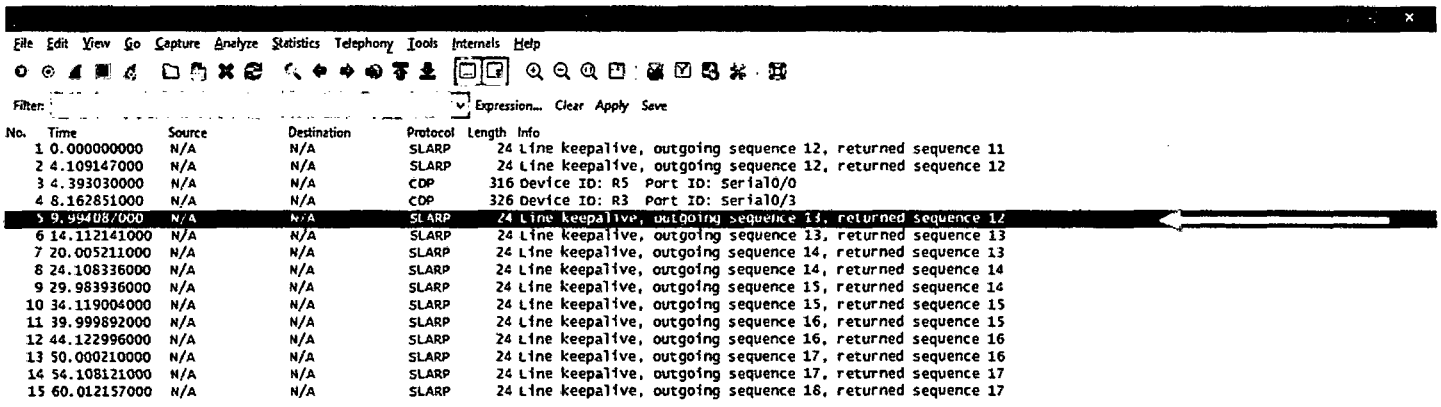


Fig. 4.1.22 Captura de paquete SLARP con Wireshark.

Información detallada sobre paquete SLARP.

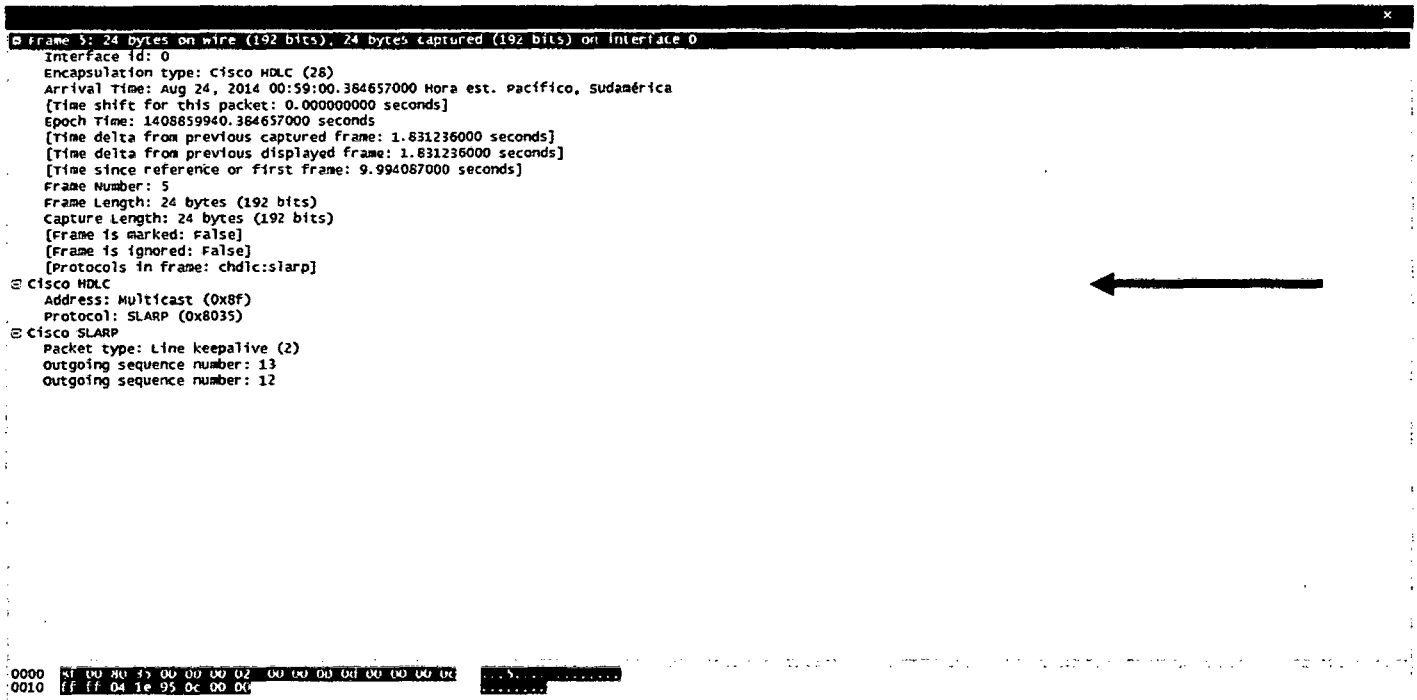


Fig. 4.1.23 Información detallada del paquete SLARP.

- Captura de paquetes ICMP.

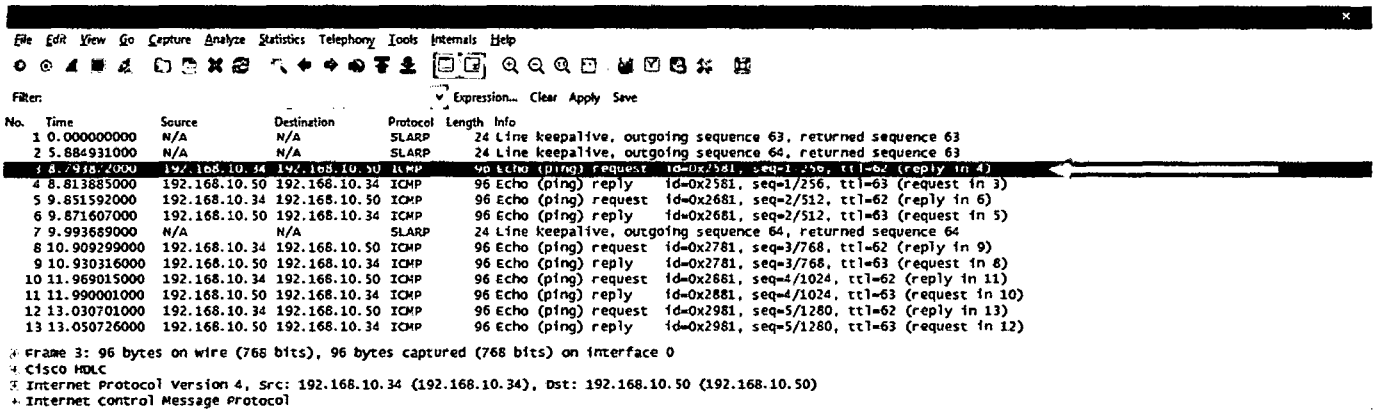


Fig. 4.1.24 Captura de paquetes ICMP con Wireshark.

Información detallada sobre paquete ICMP:

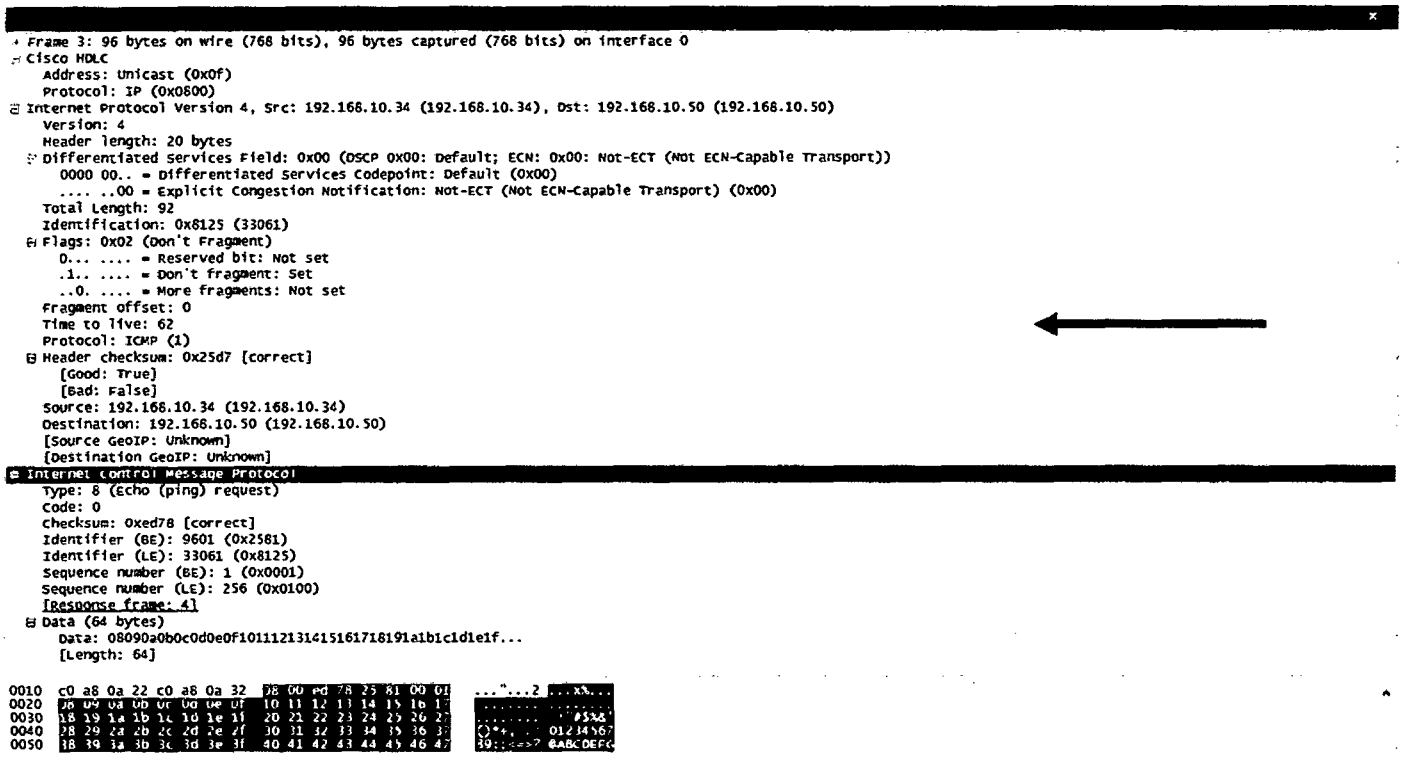


Fig. 4.1.25 Información detallada del paquete ICMP.

- Captura de paquetes CDP (Cisco Discovery Protocol), permite descubrir dispositivos Cisco que estén directamente conectados.

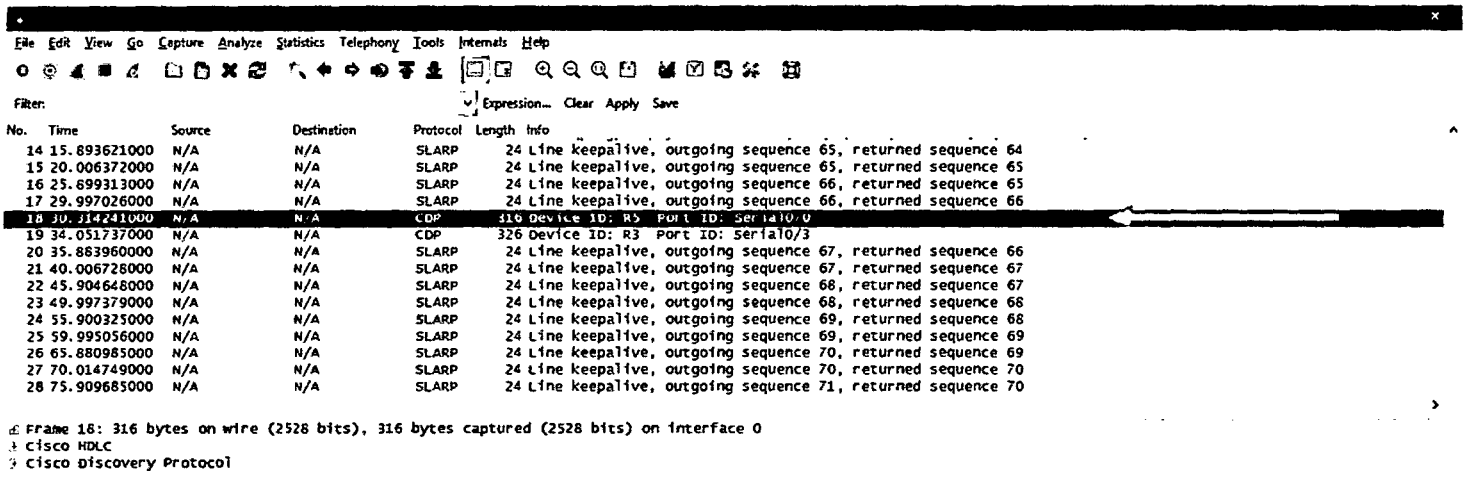


Fig. 4.1.26 Captura de paquetes CDP en Wireshark.

Información detallada sobre el dispositivo descubierto:

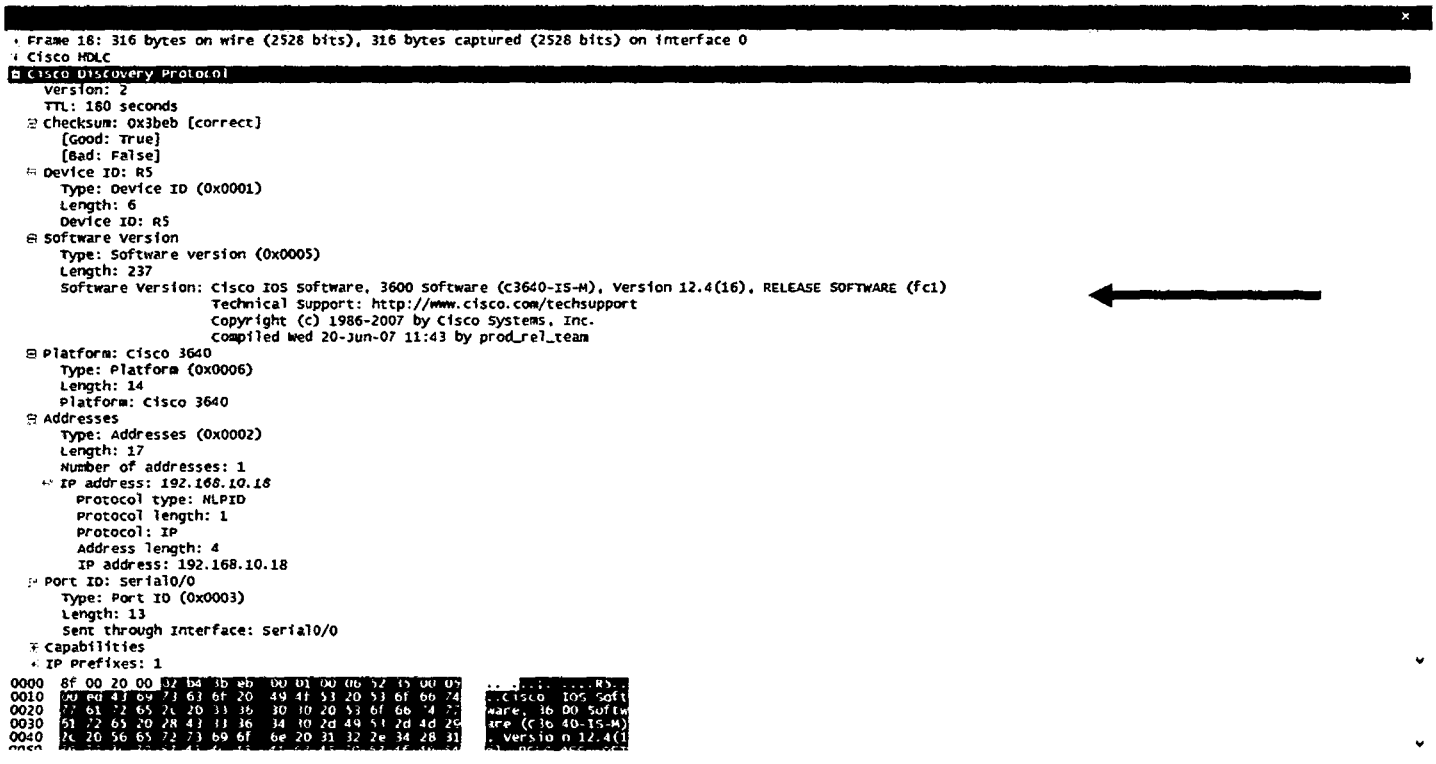


Fig. 4.1.27 Información detallada del paquete CDP.

- Captura de paquetes Traceroute, el cual se realizara desde R1 a R5.

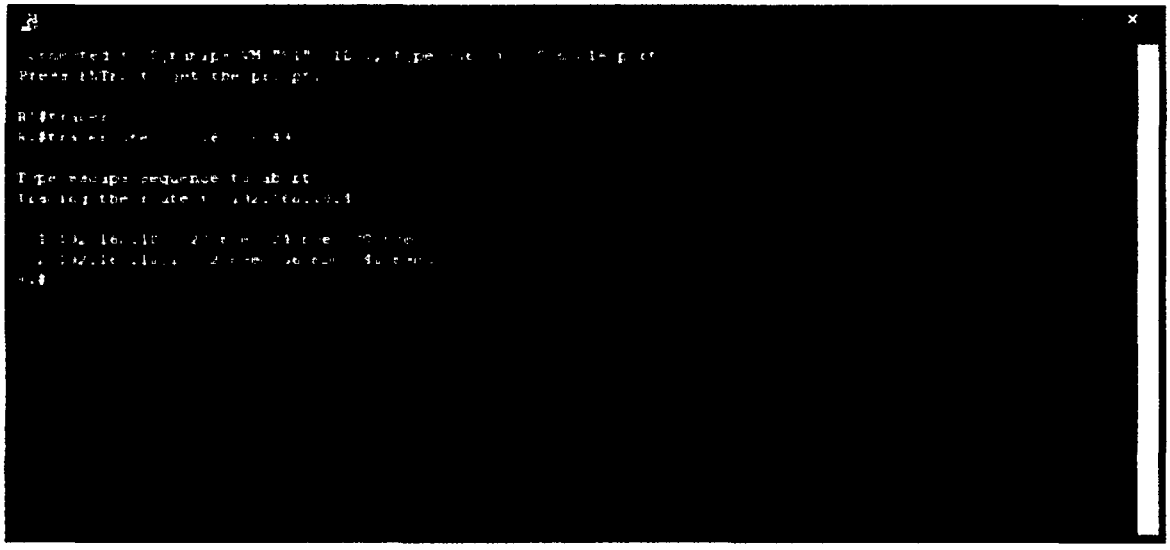


Fig. 4.1.28 Prueba de traceroute desde R1 a R5.

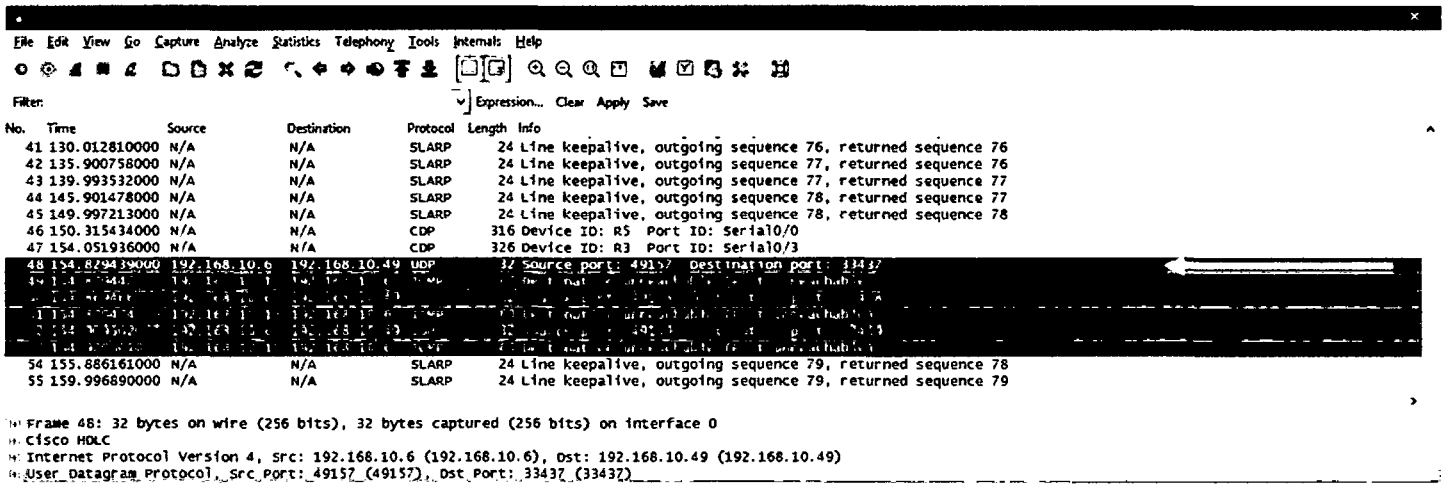


Fig. 4.1.29 Captura de paquete traceroute en Wireshark.

Información detallada sobre el paquete Traceroute.

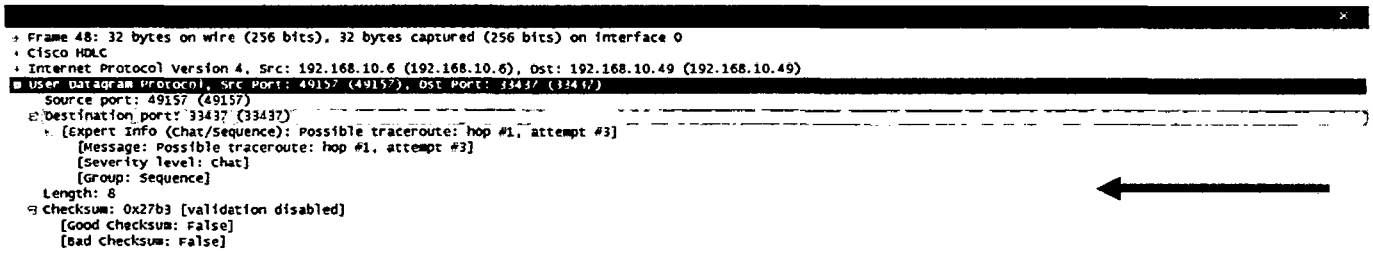
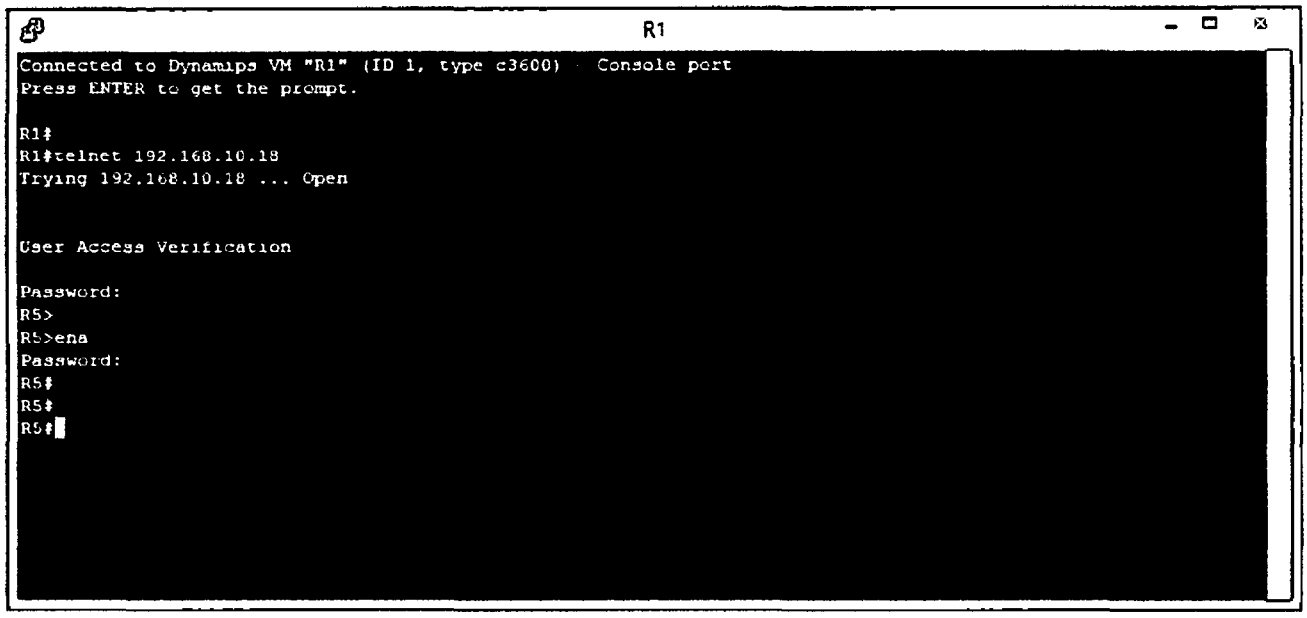


Fig. 4.1.30 Información detallada del paquete Traceroute.

- Captura de paquetes Telnet, el cual se realiza desde R1 hacia R5.



- **Fig. 4.1.31 Prueba de telnet desde R1 a R5.**

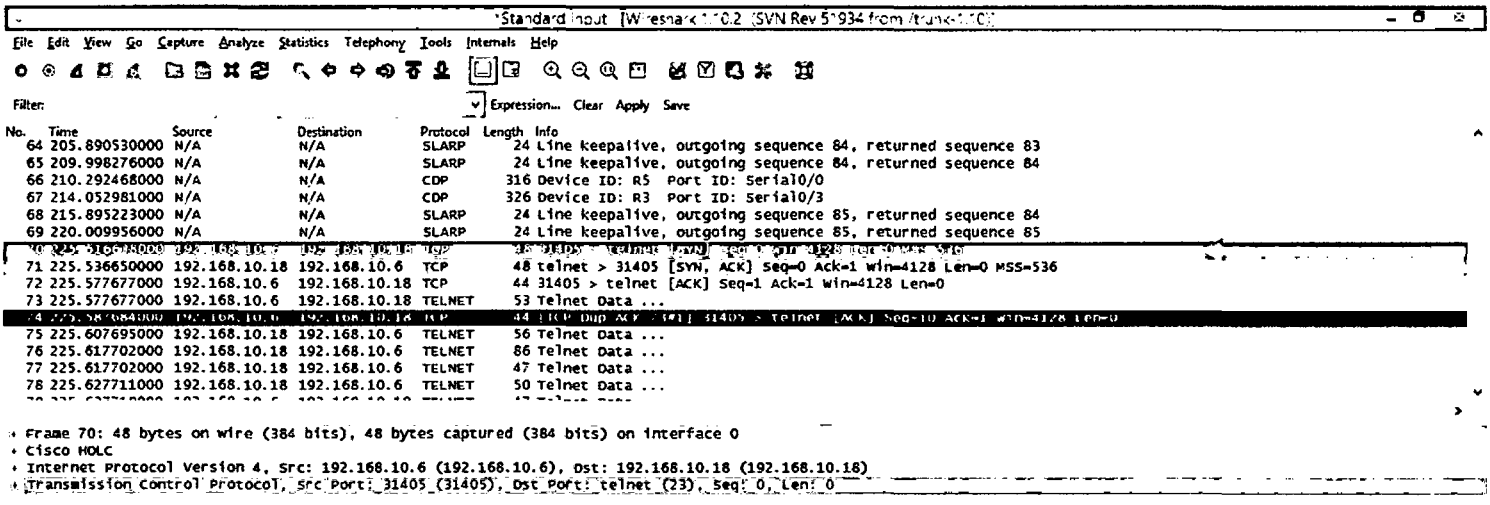


Fig. 4.1.32 Captura de paquete telnet en Wireshark.

Información detallada sobre el paquete Telnet.

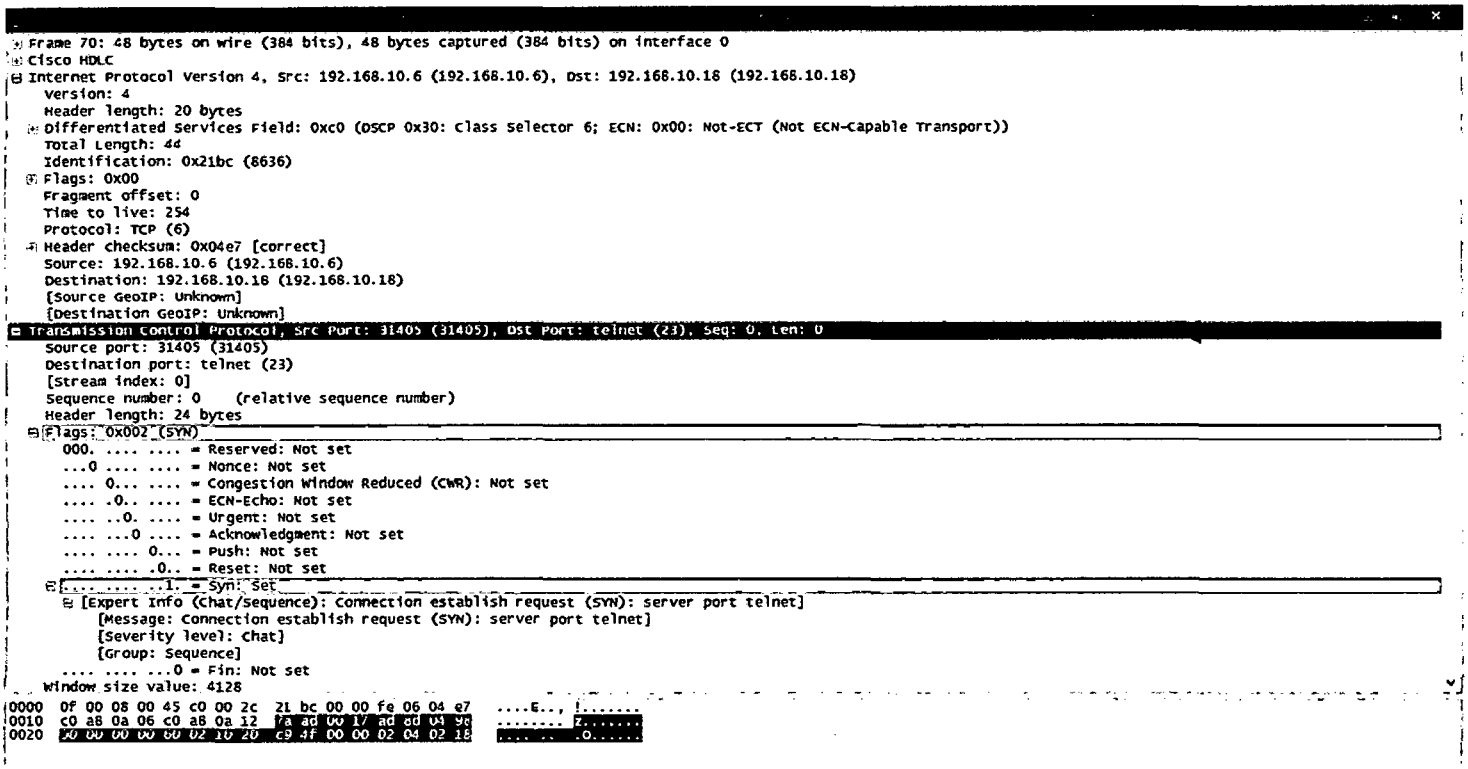


Fig. 4.1.33 Información detallada del paquete telnet.

LABORATORIO 4.2: CONFIGURACIÓN BASICA DE ENRUTAMIENTO DINAMICO CON RIPv1

REVISIÓN TEÓRICA: Para la realización de esta práctica se deberá revisar conceptos de RIP versión 1.

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet.
- Configurar una ruta dinámica con el protocolo de enrutamiento RIP v1 en todos los routers.
- Verificar el enrutamiento RIP con los comandos **show** y **debug**.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **192.170.0.0/24** para obtener el direccionamiento IP adecuado, teniendo los siguientes requisitos:

LAN R1: 20 host.
LAN R5: 8 host.

Considerando también las redes que hay entre router y router. Luego realice las configuraciones básicas en los routers y configure, después de completar la configuración pruebe la conectividad entre los dispositivos de la red y finalmente analizará el tráfico de paquetes en dicha topología.

DIAGRAMA DE TOPOLOGIA

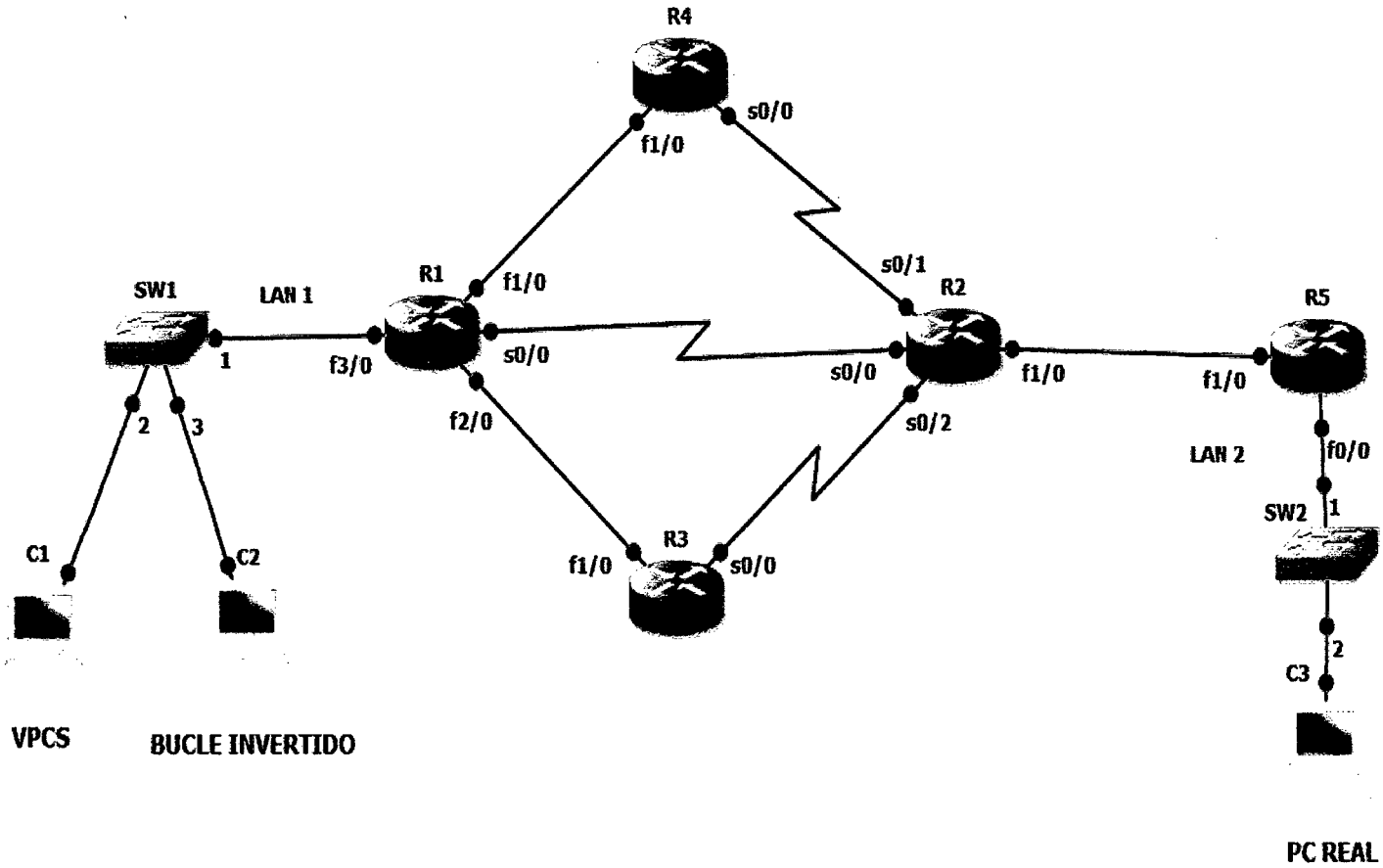


Fig. 4.2.1 Red Virtual en GNS3

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN:

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s0/0	192.170.2.1	255.255.255.0	No aplicable
	f1/0	192.170.1.1	255.255.255.0	No aplicable
	f2/0	192.170.4.1	255.255.255.0	No aplicable
	f3/0	192.170.6.1	255.255.255.0	No aplicable
R2	s0/0	192.170.2.2	255.255.255.0	No aplicable
	s0/1	192.170.3.2	255.255.255.0	No aplicable
	s0/2	192.170.5.2	255.255.255.0	No aplicable
	f1/0	192.170.7.2	255.255.255.0	No aplicable
R3	s0/0	192.170.5.1	255.255.255.0	No aplicable
	f1/0	192.170.4.2	255.255.255.0	No aplicable
R4	s0/0	192.170.3.1	255.255.255.0	No aplicable
	f1/0	192.170.1.2	255.255.255.0	No aplicable
R5	f1/0	192.170.7.1	255.255.255.0	No aplicable
	f0/0	192.170.8.1	255.255.255.0	No aplicable
C1	VPCS	192.170.6.2	255.255.255.0	192.170.6.1
C2	BUCLE INVERTIDO	192.170.6.3	255.255.255.0	192.170.6.1
PC REAL	NIC	192.170.8.2	255.255.255.0	192.170.8.1

Tabla 4.2.1 Direccionamiento IP para las Redes

TAREA 1: MONTAR LA RED EN GNS3

Montar y conectar la red igual a la del Diagrama de topología.

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

Una vez iniciado el equipo aparecerá el siguiente prompt:

Router>

Ingrese al modo privilegiado

Router>enable

Aparece el siguiente prompt

Router#

PASO 1: Establezca la configuración global del nombre de host.

En el modo exec privilegiado, ingrese al modo de configuración global:

Router# **configure terminal**

Ingrese el siguiente comando para configurar el nombre del router:

Router(config)#**hostname XXXXXX** (Escribir nombre deseado)

PASO 2: Desactive la búsqueda DNS.

Router(config)# **no ip-domain lookup**

Si escribes algo que no sea un comando de Cisco IOS o cometes un error, el router asume que ha escrito un nombre de dominio y trata de resolver lo que usted escribe, realizando una búsqueda de DNS.

PASO 3: Configure un mensaje para que se muestre al ingresar al router.

Router(config)#**banner motd %** Solo acceso a personal autorizado **%** (Puede escribir cualquier mensaje)

El símbolo % indica el inicio y final del mensaje

PASO 4: Configure las contraseñas de consola, enable secret y VTY.

Seguir los siguientes pasos:

Router(config)# **line console 0**

Router(config-line)# **password XXXXX**

Router(config-line)# **login**

Router(config-line)# **exit**

Router(config)# **enable secret XXXXX**

Router(config)# **line vty 0 4**

Router(config-line)# **password XXXXX**

Router(config-line)# **login**

Router(config-line)# **exit**

PASO 5: Sincronice los mensajes no solicitados y el resultado de la depuración con el resultado solicitado y los indicadores para las líneas de consola y de terminal virtual.

Router(config)# **line console 0**

Router(config)# **logging synchronous**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **logging synchronous**

Router(config)# **exit**

PASO 6: Configure un tiempo de espera EXEC de 10 minutos.

Router(config)# **line console 0**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

PASO 7: Guardar la configuración.

Router(config)# **copy running-config startup-config**

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET.

Aplique Los siguientes comandos:

R1:

Configuración para una interface serial DTE:

R1(config)# **interface serial 0/0**

R1(config-if)# **description conexion a R2**

R1(config-if)# **ip address 192.170.2.1 255.255.255.0**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

Configuración para una interface fasEthernet:

R1(config)# **interface fasEthernet 1/0**

R1(config-if)# **description conexion a R4**

R1(config-if)# **ip address 192.168.1.1 255.255.255.0**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface fastEthernet 2/0**

R1(config-if)# **description conexion a R3**

R1(config-if)# **ip address 192.170.4.1 255.255.255.0**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface fasEthernet 3/0**

R1(config-if)# **description conexion a LAN1**

R1(config-if)# **ip address 192.170.6.1 255.255.255.0**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R2:

Configuración para una interface serial DCE:

R2(config)# **interface serial 0/0**

R2(config-if)# **description conexion a R1**

R2(config-if)# **ip address 192.170.2.2 255.255.255.0**

R2(config-if)#**clock rate 64000**

R2(config-if)# **no shutdown**

R2(config-if)# **exit**

NOTA: Seguir los mismos pasos para la configuración de las interfaces de los demás routers.

TAREA 4: CONFIGURAR LAS RUTAS DINÁMICAS MEDIANTE EL PROTOCOLO DE ENRRUTAMIENTO RIPv1.

Paso 1: Habilite un enrutamiento dinámico.
Para habilitar un protocolo de enrutamiento dinámico, ingrese al modo de configuración global y utilice el comando **router**.
Ingrese **router?** en el indicador de configuración global para visualizar una lista de los protocolos de enrutamiento disponibles en el router.

Para habilitar RIP, ingrese el comando **router rip** en el modo de configuración global.

Configuracion de R1:

R1#**configure terminal**

R1(config)#**router rip**
R1(config-router)#

Paso 2: Ingrese direcciones de red con clase.
Una vez que se encuentre en el modo de configuración de enrutamiento, ingrese la dirección de red con clase para cada red conectada directamente por medio del comando **network**.

R1(config-router)#**network 192.170.1.0**
R1(config-router)#**network 192.170.2.0**
R1(config-router)#**network 192.170.4.0**
R1(config-router)#**network 192.170.6.0**
R1(config-router)#**passive-interface fastethernet 3/0**

R1(config-router)#**no auto-summary**
R1(config-router)#

Comando **network**:

- Habilita a RIP en todas las interfaces que pertenezcan a esta red. Ahora estas interfaces enviarán y recibirán actualizaciones RIP.
- Notifica esta red en actualizaciones de enrutamiento RIP que se envían a otros routers cada 30 segundos.

Enviar actualizaciones desde la interfaz desperdicia ancho de banda y recursos de procesamiento de todos los dispositivos de la LAN. Además, notificar actualizaciones en una red de broadcast es un riesgo para la seguridad. Las actualizaciones RIP pueden interceptarse con software analizador de protocolos. Las actualizaciones de enrutamiento pueden modificarse y enviarse de regreso al router, dañando la tabla del router con métricas falsas que orientan mal el tráfico. El comando passive-interface fastethernet 1/0 se utiliza para deshabilitar el envío de actualizaciones RIPv1 a la interfaz.
Al finalizar la configuración RIP, regrese al modo EXEC privilegiado y guarde la configuración actual para la NVRAM.

R1(config-router)#**end**
%SYS-5-CONFIG_I: Configured from console by console
R1#**copy run start**

Paso 3: Configure RIP en el router R3 por medio de los comandos router rip y network.

R3(config)#**router rip**
R3(config-router)#**network 192.170.4.0**
R3(config-router)#**network 192.170.5.0**
R3(config-router)#**no auto-summary**
R3(config-router)#**end**
%SYS-5-CONFIG_I: Configured from console by console
R3#**copy run start**

Al finalizar la configuración RIP, regrese al modo EXEC privilegiado y guarde la configuración actual para la NVRAM.

NOTA: Para eliminar las configuraciones RIP de cada router use el comando de configuración global **no router rip**. Esto eliminará todos los comandos de configuración RIP, incluso los comandos **network**.

R1(config)#**no router rip**

NOTA: Seguir los mismos pasos para los routers R2, R4 y R5.

TAREA 5: CONFIGURAR LOS EQUIPOS DE HOST.

Configurar las direcciones IP y gateways por defecto como se indican en la tabla de direccionamiento de las interfaces Ethernet de C1, C2 (VPCS) y PC REAL.

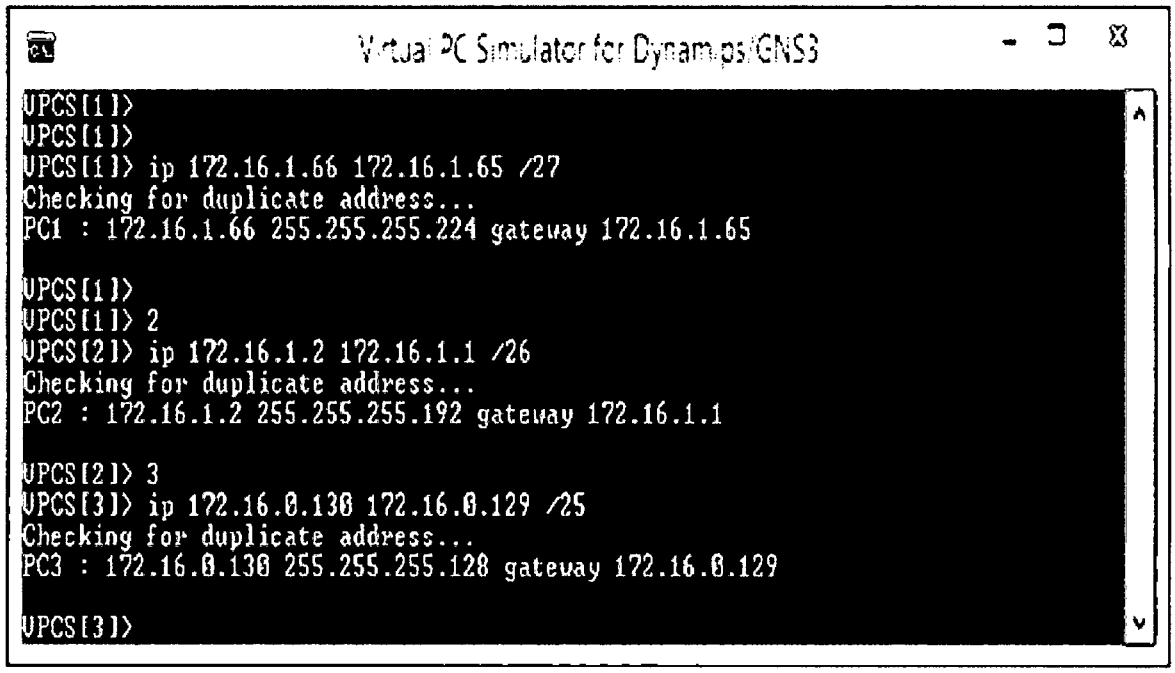


Fig. 4.2.2 Configuración de la Direccion IP de las VPCS

TAREA 6: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

PASO 1: Verificar el direccionamiento IP y las interfaces.

R1# **show ip interface brief**

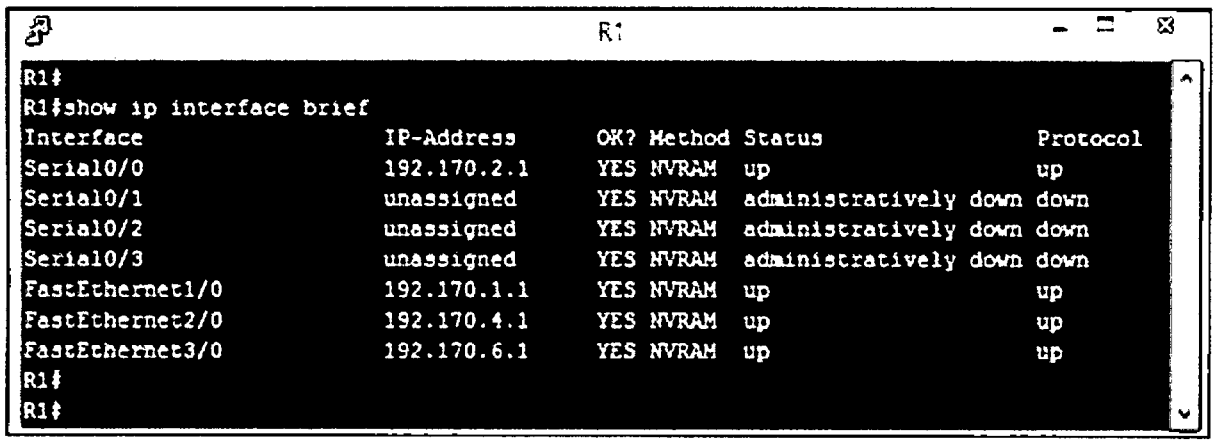


Fig. 4.2.2 Tabla ip de Interfaces Activas de R1

R2(config)# **show ip interface brief**

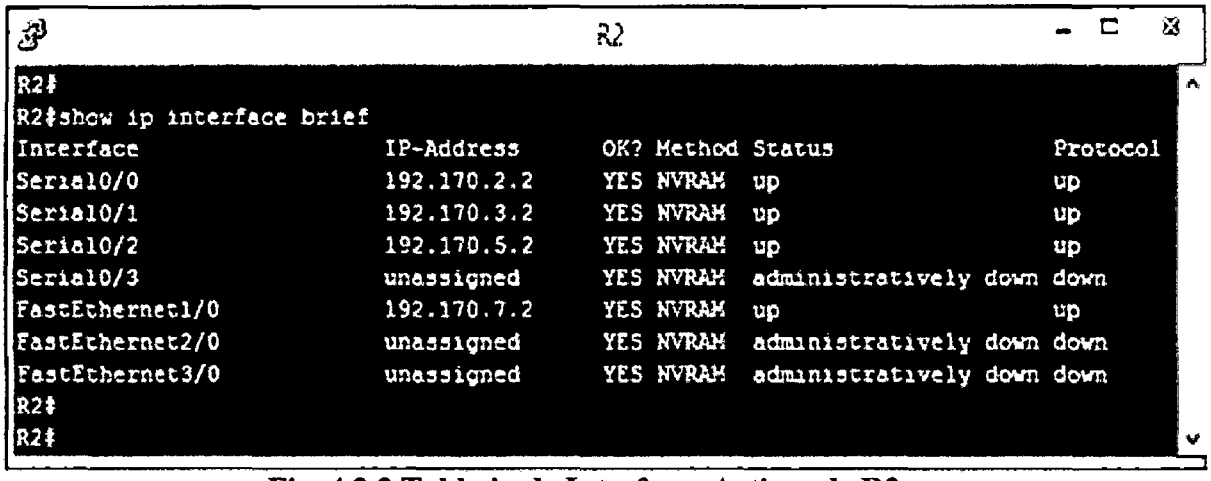


Fig. 4.2.3 Tabla ip de Interfaces Activas de R2

Nota: Verificar que las interfaces de los demás routers tengan la adecuada dirección IP y estén activas.

PASO 2: Verificar la configuración de los router. Use los comandos **show ip route** para verificar el contenido de la tabla de enrutamiento.

R1# **show ip route**

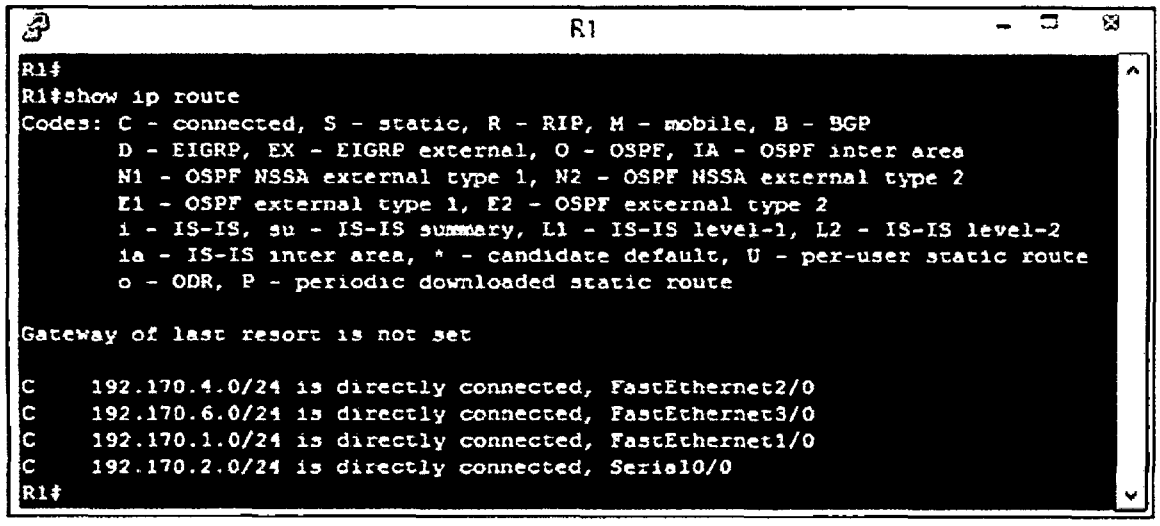


Fig. 4.2.4 Tabla de Enrutamiento de R1 antes de configurar el protocolo RIP

R1#**show ip route**

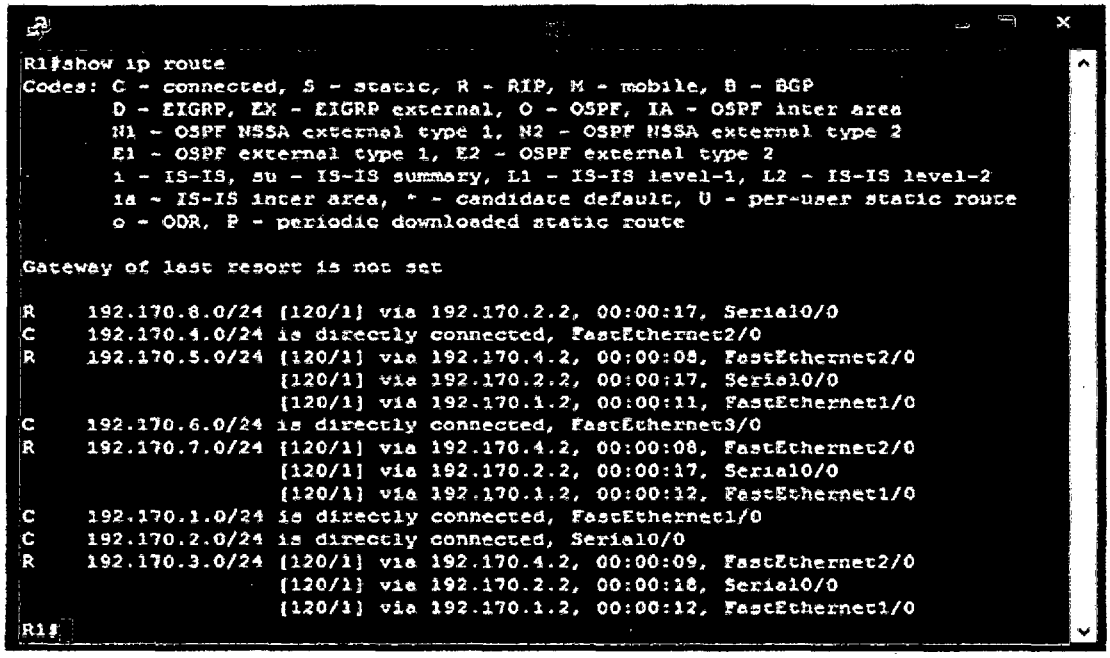


Fig. 4.2.5 Tabla de Enrutamiento de R1

Las rutas reveladas a través de RIP se codifican con una **R** en la tabla de enrutamiento. Si las tablas no convergen como se muestra a continuación, resuelva los problemas de configuración.

R2#**show ip route**

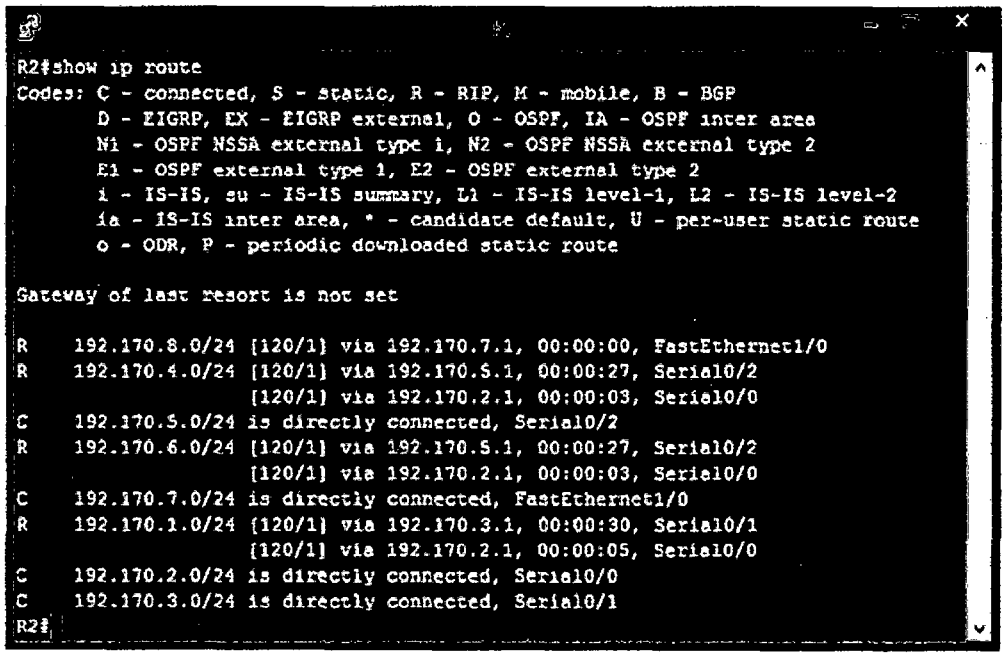


Fig. 4.2.6 Tabla de Enrutamiento de R2

PASO 3: Utilice el comando ***show ip protocols*** para visualizar la información acerca de los procesos de enrutamiento.

El comando **show ip protocols** se puede utilizar para visualizar información acerca de los procesos de enrutamiento que se producen en el router. Se puede utilizar este resultado para verificar los parámetros RIP para confirmar que:

- El uso del enrutamiento RIP está configurado.
- Las interfaces correctas envían y reciben las actualizaciones RIP.
- El router notifica las redes correctas.
- Los vecinos RIP están enviando actualizaciones.

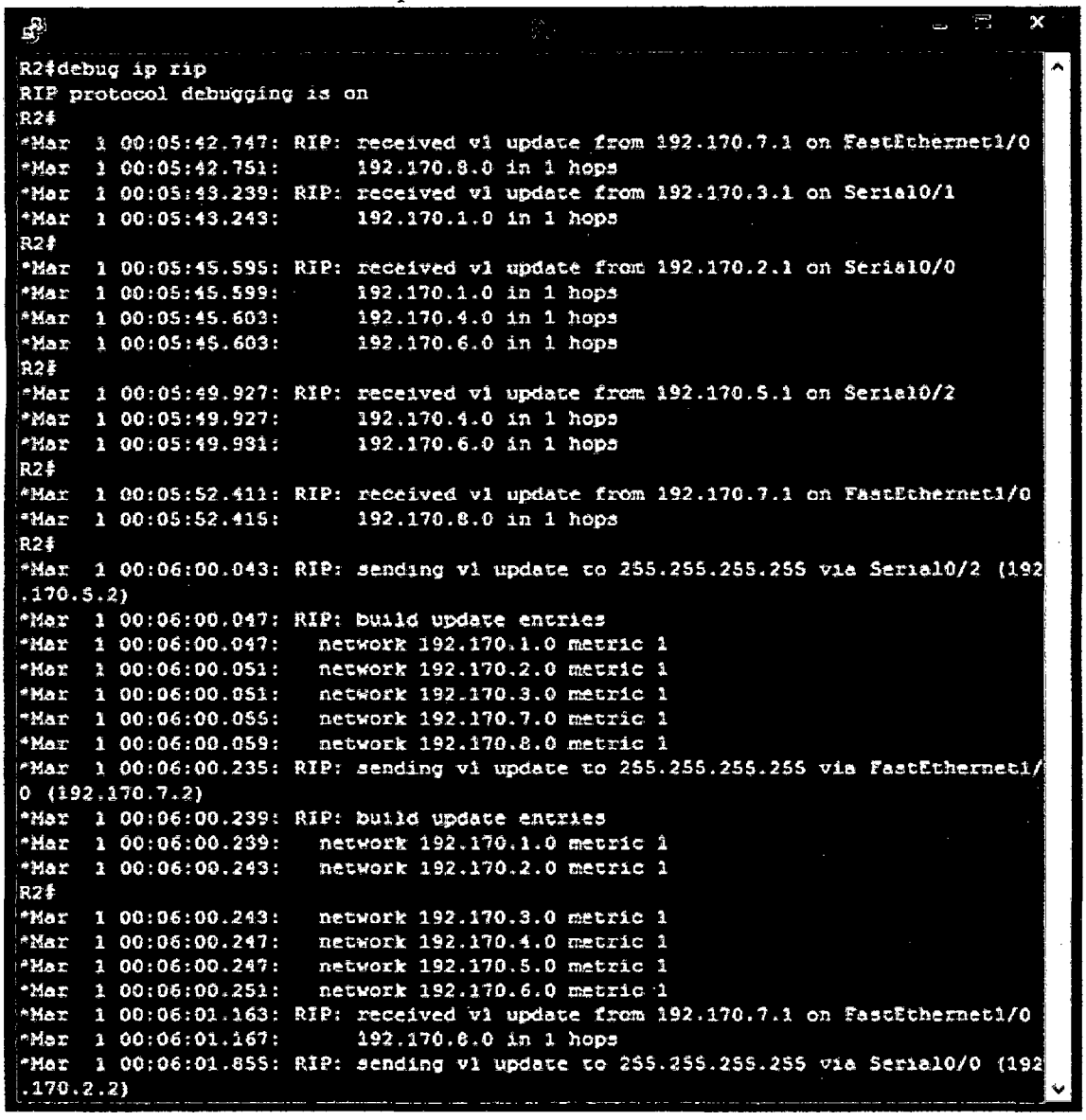
R2#**show ip protocols**

Fig. 4.2.7 Procesos de Enrutamiento

R1 sí está configurado con RIP. R1 está enviando y recibiendo actualizaciones RIP en FastEthernet1/0, FastEthernet2/0, FastEthernet3/0 y Serial0/0. R1 está notificando las redes 192.170.1.0, 192.170.2.0, 192.170.4.0 y 192.170.6.0. R1 tiene una fuente de información de enrutamiento. R2, R3, R4 y R5 le están enviando actualizaciones a R1.

PASO 4: Utilice el comando ***debug ip rip*** para visualizar los mensajes RIP que se envían y reciben.

Las actualizaciones rip se envían cada 30 segundos, por lo que deberá esperar para visualizar la información de depuración.



```
R2#debug ip rip
RIP protocol debugging is on
R2#
*Mar  1 00:05:42.747: RIP: received v1 update from 192.170.7.1 on FastEthernet1/0
*Mar  1 00:05:42.751:      192.170.8.0 in 1 hops
*Mar  1 00:05:43.239: RIP: received v1 update from 192.170.3.1 on Serial0/1
*Mar  1 00:05:43.243:      192.170.1.0 in 1 hops
R2#
*Mar  1 00:05:45.595: RIP: received v1 update from 192.170.2.1 on Serial0/0
*Mar  1 00:05:45.599:      192.170.1.0 in 1 hops
*Mar  1 00:05:45.603:      192.170.4.0 in 1 hops
*Mar  1 00:05:45.603:      192.170.6.0 in 1 hops
R2#
*Mar  1 00:05:49.927: RIP: received v1 update from 192.170.5.1 on Serial0/2
*Mar  1 00:05:49.927:      192.170.4.0 in 1 hops
*Mar  1 00:05:49.931:      192.170.6.0 in 1 hops
R2#
*Mar  1 00:05:52.411: RIP: received v1 update from 192.170.7.1 on FastEthernet1/0
*Mar  1 00:05:52.415:      192.170.8.0 in 1 hops
R2#
*Mar  1 00:06:00.043: RIP: sending v1 update to 255.255.255.255 via Serial0/2 (192
.170.5.2)
*Mar  1 00:06:00.047: RIP: build update entries
*Mar  1 00:06:00.047:   network 192.170.1.0 metric 1
*Mar  1 00:06:00.051:   network 192.170.2.0 metric 1
*Mar  1 00:06:00.051:   network 192.170.3.0 metric 1
*Mar  1 00:06:00.055:   network 192.170.7.0 metric 1
*Mar  1 00:06:00.059:   network 192.170.8.0 metric 1
*Mar  1 00:06:00.235: RIP: sending v1 update to 255.255.255.255 via FastEthernet1/
0 (192.170.7.2)
*Mar  1 00:06:00.239: RIP: build update entries
*Mar  1 00:06:00.239:   network 192.170.1.0 metric 1
*Mar  1 00:06:00.243:   network 192.170.2.0 metric 1
R2#
*Mar  1 00:06:00.243:   network 192.170.3.0 metric 1
*Mar  1 00:06:00.247:   network 192.170.4.0 metric 1
*Mar  1 00:06:00.247:   network 192.170.5.0 metric 1
*Mar  1 00:06:00.251:   network 192.170.6.0 metric 1
*Mar  1 00:06:01.163: RIP: received v1 update from 192.170.7.1 on FastEthernet1/0
*Mar  1 00:06:01.167:      192.170.8.0 in 1 hops
*Mar  1 00:06:01.855: RIP: sending v1 update to 255.255.255.255 via Serial0/0 (192
.170.2.2)
```

Fig. 4.2.8 Mensajes del Protocolo RIP

El resultado de la depuración muestra que R1 recibe una actualización de los otros routers. Observe cómo esta actualización incluye todas las redes que R1 aún no tiene en su tabla de enrutamiento. Debido a que la interfaz FastEthernet3/0 pertenece a la red 192.170.6.0 configurada en RIP, R1 crea una actualización para enviar a esa interfaz. La actualización incluye todas las redes conocidas para R1, excepto la red de la interfaz, lo mismo ocurre para las otras interfaces. Por último, R1 crea una actualización para enviar a los demás routers. Debido a este horizonte dividido, R1 incluye en la actualización las redes 192.170.1.0, 192.170.2.0, 192.170.4.0 y 192.170.6.0.

Para detener el resultado de la depuración configure el comando ***undebug all*** en el router.

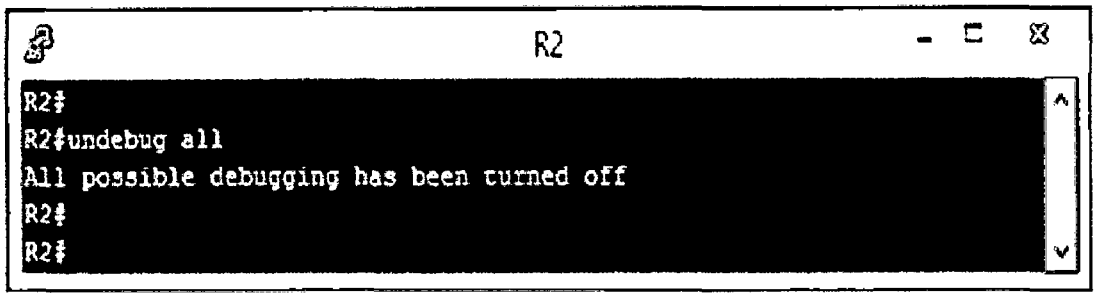


Fig. 4.2.9 Detener Mensajes del Protocolo RIP

PASO 5: Verificar que hay conectividad completa en la red.

Use el comando **ping** para verificar la conectividad.

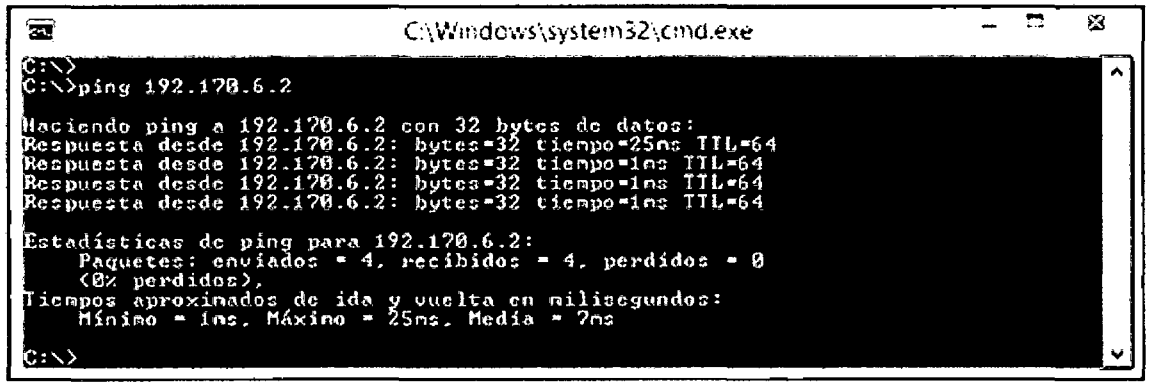


Fig. 4.2.10 Comprobación de conectividad entre C2 y C1

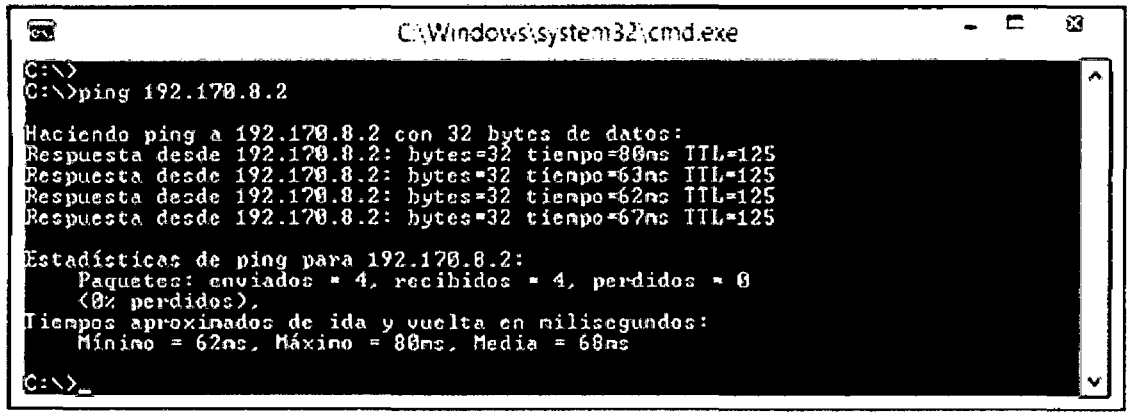


Fig. 4.2.11 Comprobación de conectividad entre C2 y PC REAL

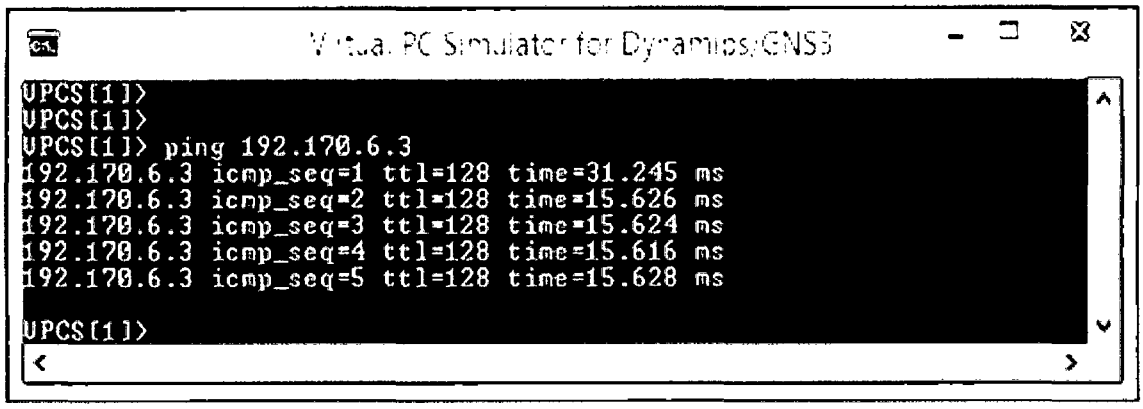


Fig. 4.2.12 Comprobación de conectividad entre C1 y C2

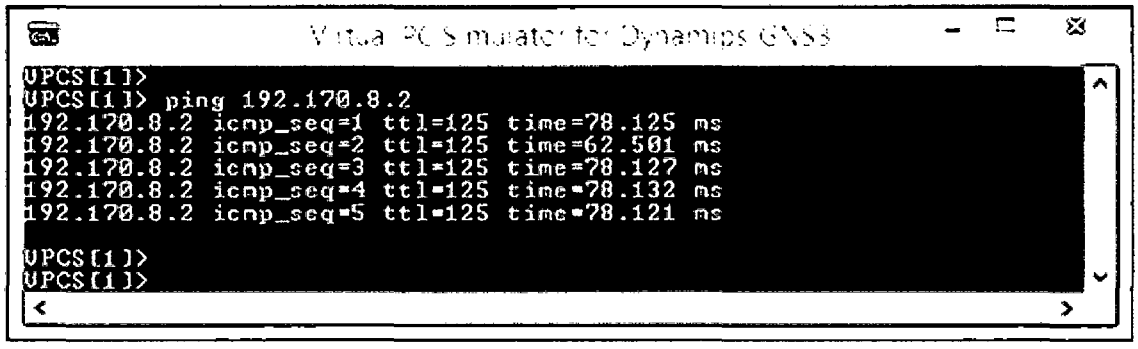


Fig. 4.2.13 Comprobación de conectividad entre C1 y PC REAL

TAREA 8: ANALIS DEL TRAFICO DE PAQUETES

PASO 1: Medición de la Latencia

Para la medición de la latencia se realizó 10 muestras sucesivas de 100 ping desde el C2 (Bucle invertido) hacia la PC REAL considerando un tamaño de trama de 64, 512 y 1518 bytes como se especifica en el RFC 2544.

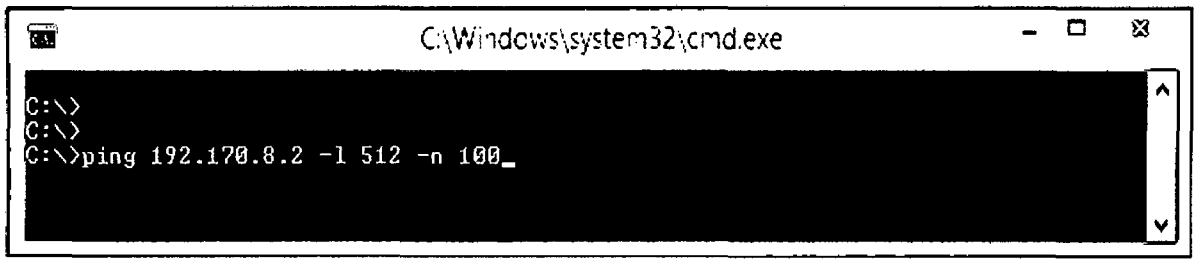


Fig. 4.2.14 Forma de medición de la Latencia

En la Figura 4.2.16 se puede observar el envío de 100 ping con una trama de 512 hacia la dirección 192.170.8.2.

En las Tablas posteriores se detallan los valores de la Latencia que se ha obtenido una vez realizadas todas las muestras.

LATENCIA											
Tamaño de Trama (bytes)	64										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	37	34	36	35	50	56	37	37	59	58	43.9
Tiempo Máximo (ms)	152	147	134	185	229	191	172	182	163	165	172
Tiempo Promedio (ms)	100	80	81	88	107	109	103	98	102	105	97.3

Tabla 4.2.2 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	512										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	70	69	40	56	56	71	41	43	70	43	55.9
Tiempo Máximo (ms)	171	187	196	180	197	291	202	233	177	300	213.4
Tiempo Promedio (ms)	103	114	114	102	109	115	104	117	106	105	109.3

Tabla 4.2.3 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1518										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	56	63	74	56	59	63	72	75	65	61	64.4
Tiempo Máximo (ms)	218	199	251	185	262	262	328	325	253	234	251.7
Tiempo Promedio (ms)	119	118	111	109	116	111	127	113	114	110	114.8

Tabla 4.2.4 Datos obtenidos para una trama de 1518 bytes.

LATENCIA			
Tamaño de Trama (bytes)	**64**	**512**	**1518**
Tiempo Mínimo (ms)	**43.9**	**55.9**	**64.4**
Tiempo Máximo (ms)	**172**	**213.4**	**251.7**
Tiempo Promedio (ms)	**97.3**	**109.3**	**114.8**

Tabla 4.2.5 Comparación de datos obtenidos de las diferentes tramas.

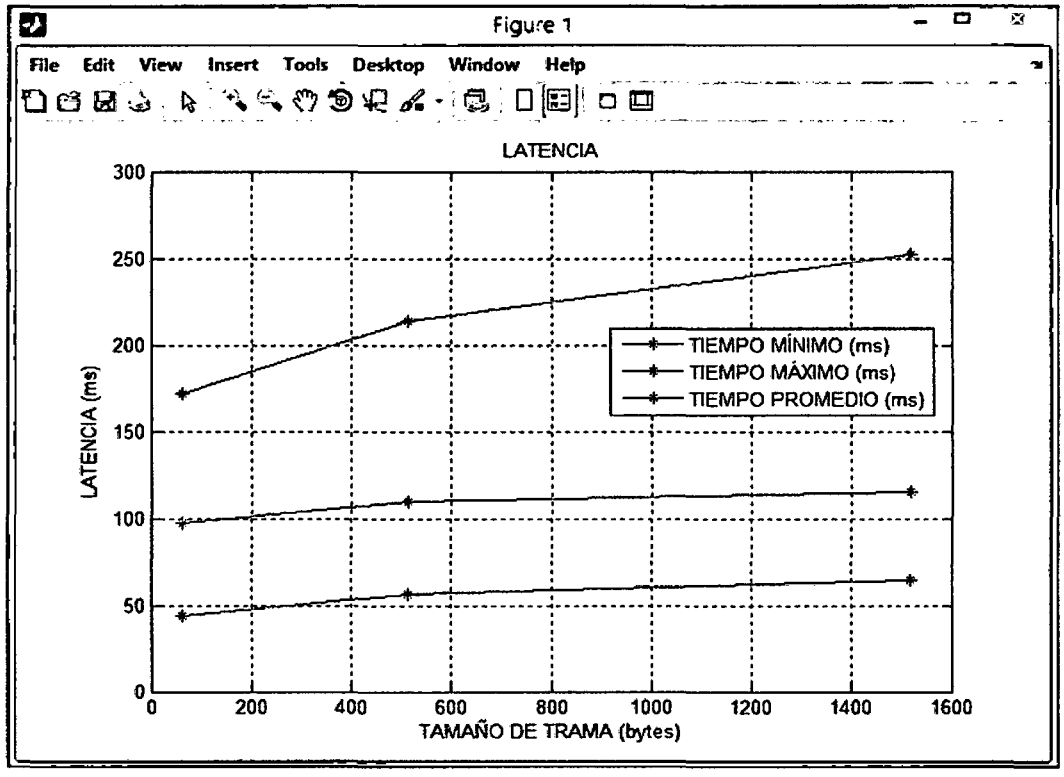


Fig. 4.2.15 Datos representados gráficamente de la variación de la latencia.

De acuerdo con los datos obtenidos, se puede observar claramente que los valores mínimo (color azul), máximo (color rojo) y promedio (color verde) de la latencia de la red se incrementan conforme se envía una trama de longitud mayor, en este caso con la trama de 1518 bytes se obtiene una latencia promedio de 114.8 ms a diferencia de una trama de 64 bytes con 97.3 ms.

PASO 2: Medición del Throughput

Para la medición del Throughput y Jitter se envió una cantidad de tramas a velocidades diferentes durante 20 segundos, hasta encontrar la máxima cantidad de tramas recibidas sin que se produzcan perdidas de las mismas en el router y PC REAL. Como se utilizó Jperf el cliente será el encargado de enviar los paquetes y el servidor los recibirá, indicando la cantidad de paquetes que llegaron correctamente considerando un tamaño del paquete UDP de 750, 1125, 1500 y 1470 (default) bytes, tal como se especifica en el RFC 768.

Configuración del Jperf como servidor para medir Throughput:

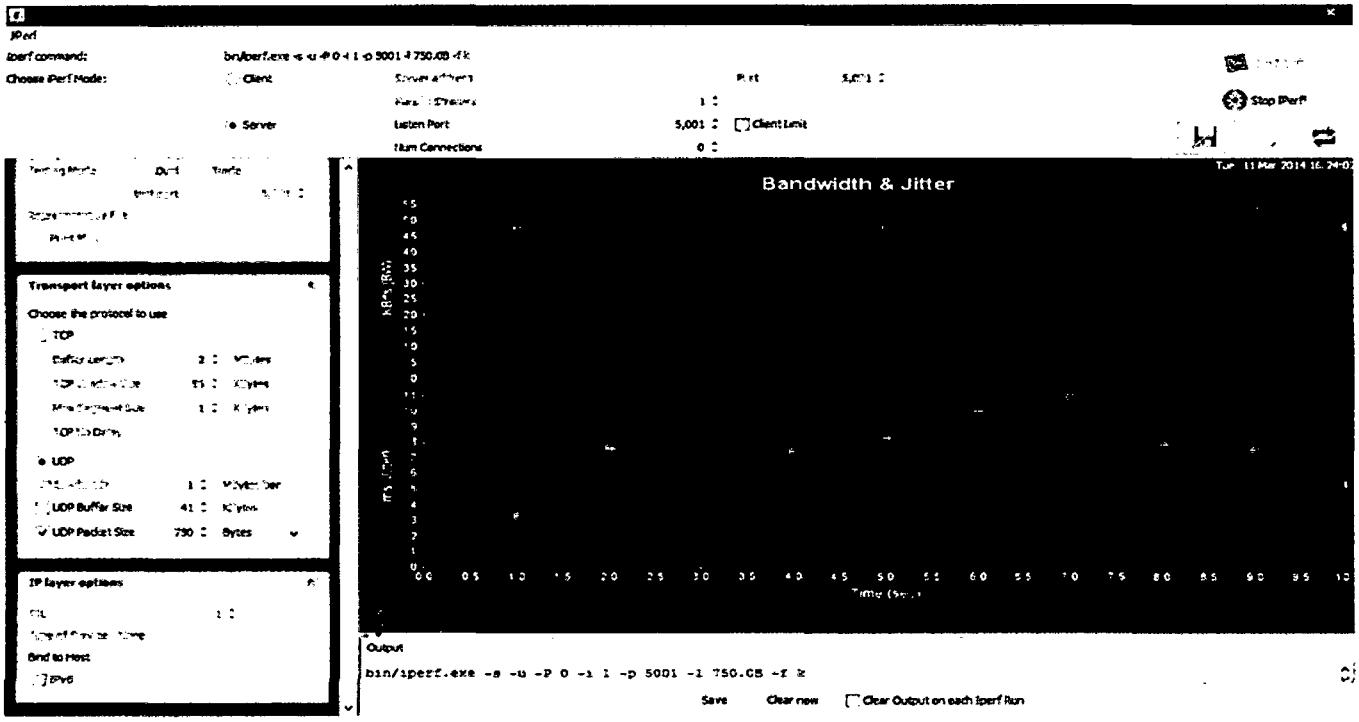


Fig. 4.2.16 Gráfico del Bandwidth y Jitter.

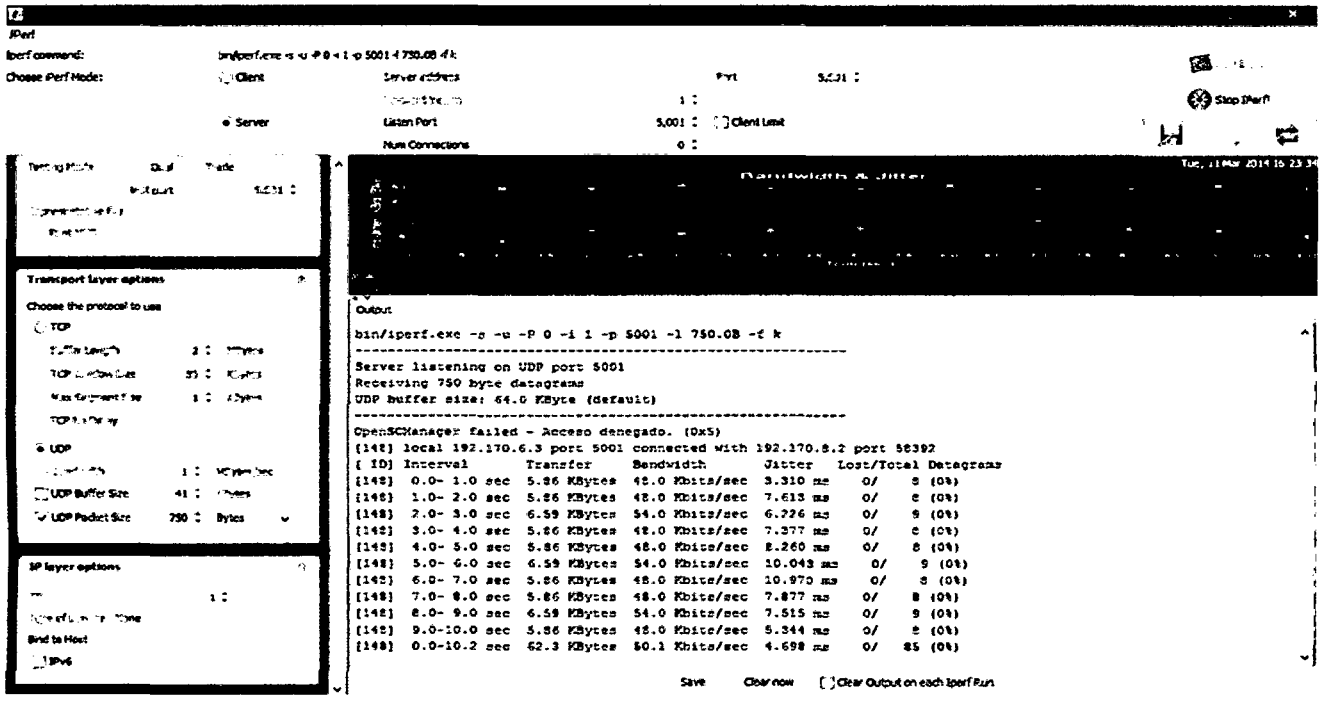


Fig. 4.2.17 Configuración del Jperf como Servidor para medir Jitter.

Configuración del Jperf como cliente para medir Throughput:

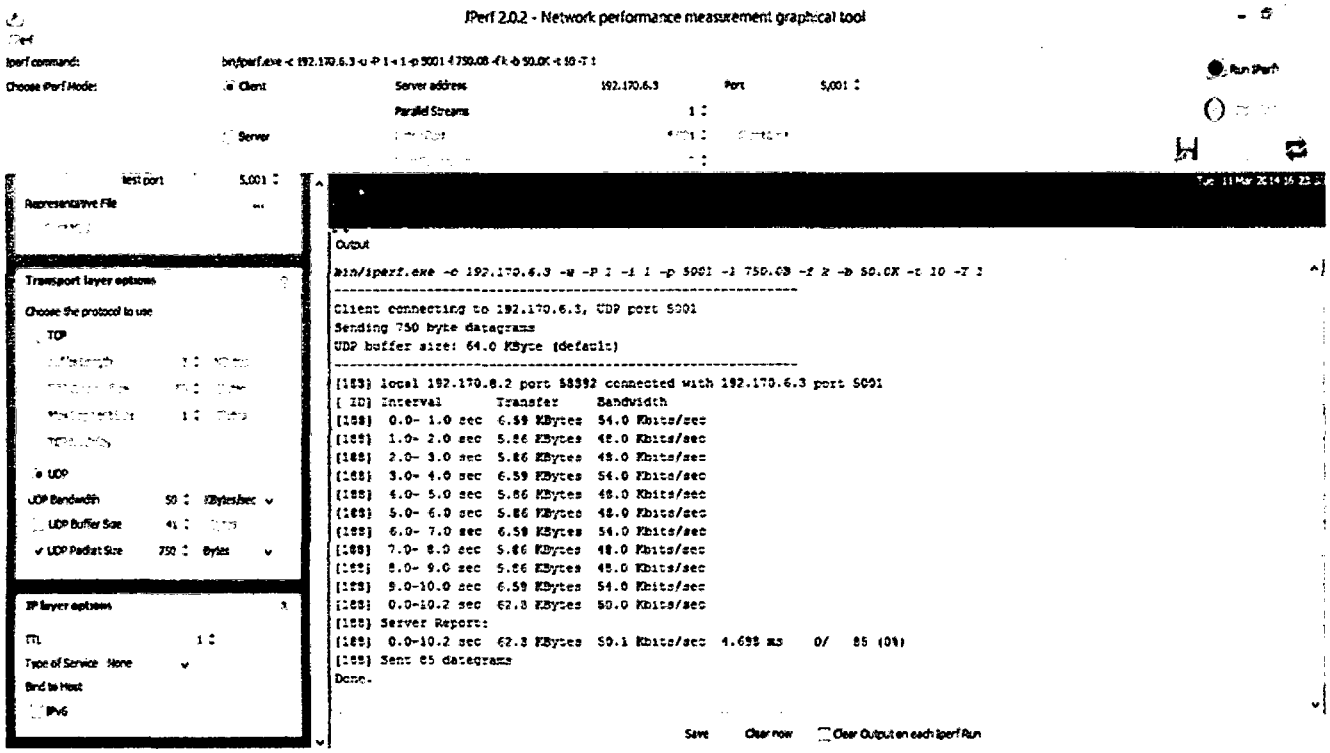


Fig. 4.2.18 Configuración del Jperf como Cliente para medir Throughput

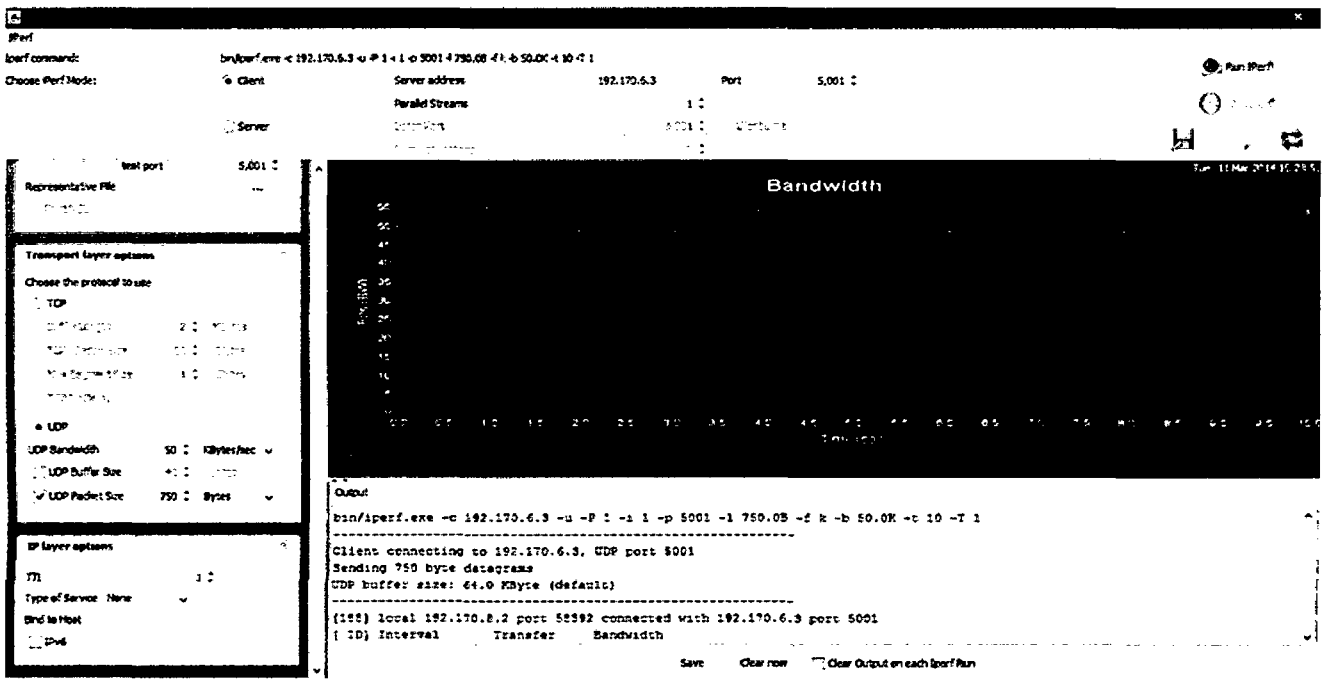


Fig. 4.2.19 Gráfico del Ancho de Banda en Jperf

En las siguientes Tablas se detalla los valores del Throughput obtenidos una vez realizada todas las muestras.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (kbps)	**50**	**50**	**50**
Velocidad de Rx (kbps)	**49.8**	**50**	**45.8**
Tramas Transmitidas	**85**	**57**	**43**
Tramas Recibidas	**85**	**57**	**43**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**8**	**6**	**4**

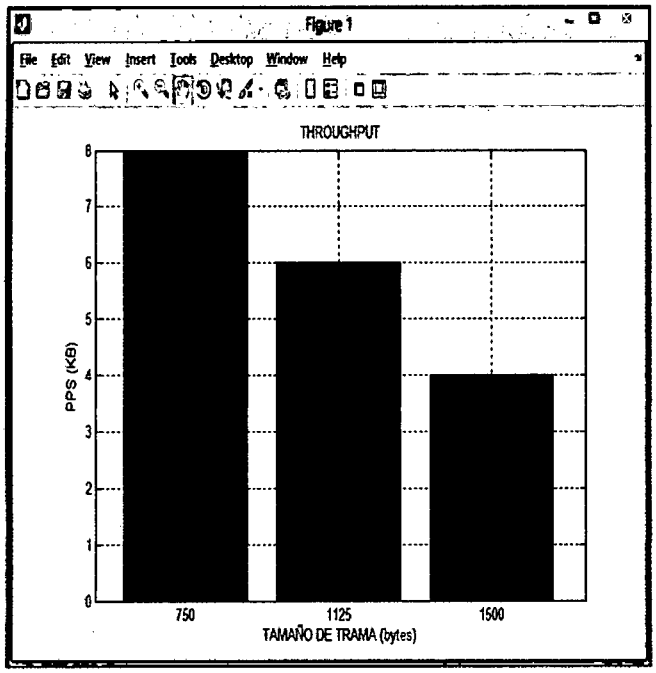
Tabla 4.2.6 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (kbps)	**20**	**50**	**100**
Velocidad de Rx (kbps)	**20**	**43.6**	**89.9**
Tramas Transmitidas	**18**	**44**	**86**
Tramas Recibidas	**18**	**44**	**86**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**2**	**5**	**5**

Tabla 4.2.7 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**0.5**	**1**	**2**
Velocidad de Rx (Mbps)	**0.49**	**0.924**	**1.21**
Tramas Transmitidas	**424**	**849**	**1701**
Tramas Recibidas	**424**	**849**	**1598**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**103 (6.1%)**
Tramas Recibidas (pps)	**43**	**85**	**170**

Tabla 4.2.8 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.



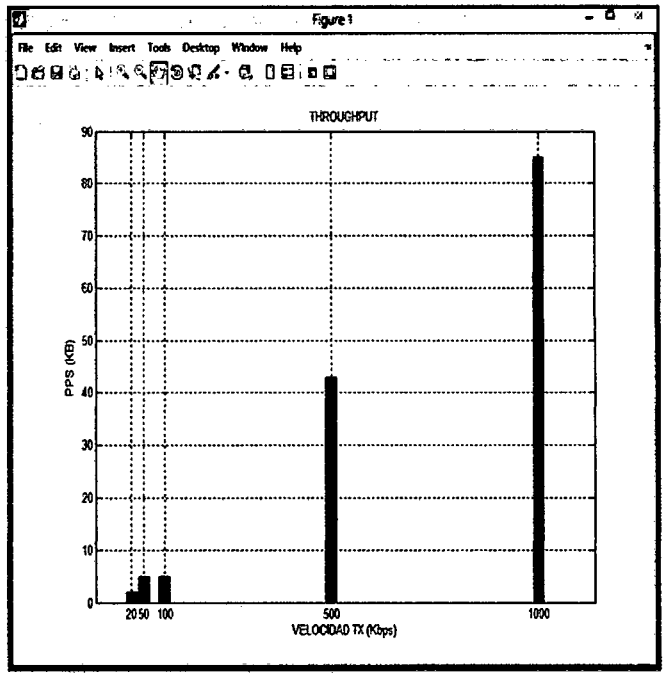


Fig. 4.2.20 PPS vs. Tamaño de Trama

Fig. 4.2.21 PPS vs. Velocidad Tx

En la figura 4.2.18, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 750 bytes, 1125 bytes y 1500 bytes los cuales han utilizado una velocidad de Tx constante de 50 kbps, en la gráfica se puede observar claramente que al enviar una trama de 750 bytes se envía 8 pps, con una trama de 1125 se envía 6 pps y con una trama de 1500 se envía 4 pps.

Mientras en la figura 4.2.19, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 1470 bytes los cuales han utilizado una velocidad de Tx variada desde 20 kbps hasta 1 Mbps sin que se produzcan perdidas en el envío, en la gráfica se observa que a 20 kbps se envían 2 pps, en cambio a 1 Mbps se obtiene 85 pps.

PASO 3: Medición del Jitter

Para la medición se envió datos UDP de longitud variable a velocidades diferentes de Throughput obtenida anteriormente durante 20 segundos. Como se utilizó anteriormente Jperf el cliente será el encargado de enviar los datos y el servidor los recibirá, indicando los valores de Jitter obtenidos durante la transmisión de los datos.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (kbps)	**50**	**50**	**50**
Velocidad de Rx (kbps)	**49.8**	**50**	**45.8**
Tramas Transmitidas	**85**	**57**	**43**
Tramas Recibidas	**85**	**57**	**43**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**4.698**	**9.068**	**13.16**

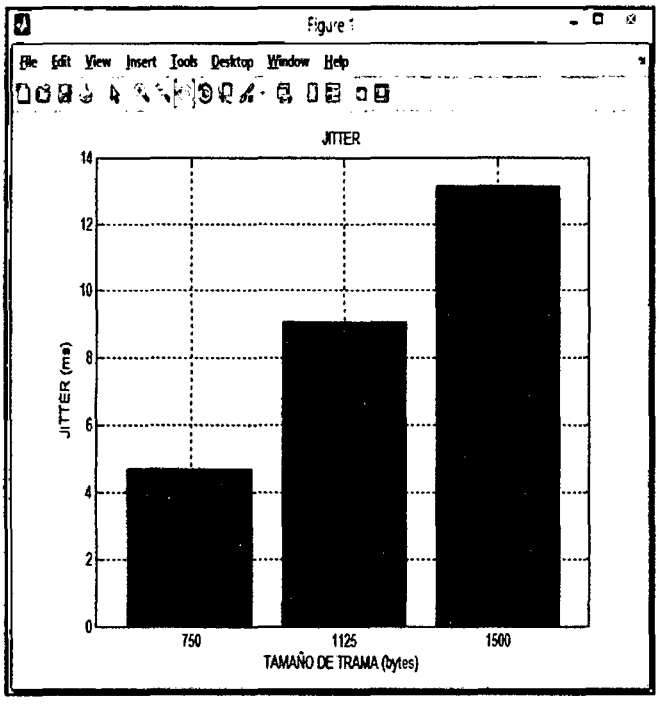
Tabla 4.2.9 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (kbps)	**20**	**50**	**100**
Velocidad de Rx (kbps)	**20**	**43.6**	**89.9**
Tramas Transmitidas	**18**	**44**	**86**
Tramas Recibidas	**18**	**44**	**86**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**6.898**	**20.713**	**20.9**

Tabla 4.2.10 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**0.5**	**1**	**2**
Velocidad de Rx (Mbps)	**0.5**	**0.924**	**1.21**
Tramas Transmitidas	**426**	**851**	**1701**
Tramas Recibidas	**426**	**851**	**1598**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**103 (6.1%)**
Jitter (ms)	**22.935**	**23.441**	**25.009**

Tabla 4.2.11 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.



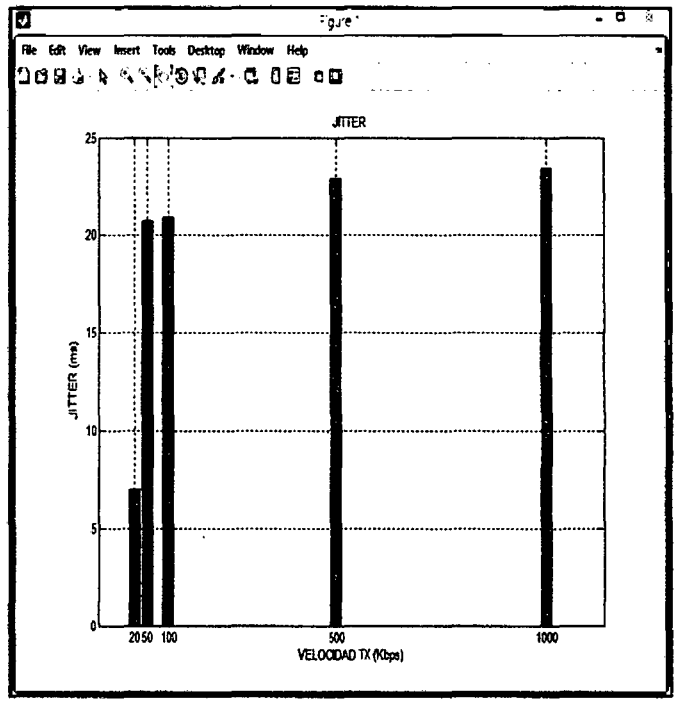


Fig. 4.2.22 Jitter vs. Tamaño de Trama

Fig. 4.2.23 Jitter vs. Velocidad Tx

En la figura 4.2.20 se observa los valores del Jitter obtenidos al enviar diferentes tamaños de paquete UDP como 750, 1125 y 1500 bytes utilizando una velocidad de Tx constante de 50 kbps, se puede observar claramente que con una trama de 750 bytes se tiene un Jitter de 4.69 ms a diferencia de la trama de 1500 bytes en la cual se tiene un Jitter de 13.16 ms.

En la figura 4.2.21, se observa los valores del Jitter obtenidos al enviar paquetes UDP de 1470 bytes utilizando una velocidad de Tx que varía entre los 20 kbps y los 2 Mbps, se puede observar claramente que con una velocidad Tx de 20 kbps se tiene un Jitter de 3. 01 ms a diferencia que a una velocidad Tx de 1 Mbps en la cual se tiene un Jitter de 23.44 ms.

En la tabla de medición de valores de Throughput y Jitter se observa que la topología de red construida en gns3 para la implementación del laboratorio RIPv1 nos soporta una velocidad de Tx máxima de 1 Mbps sin que haya perdidas en el envió de tramas desde la C1 hasta la Pc Real, superado esa velocidad de Tx en esta topología obtendremos demasiadas perdidas de tramas, como observamos que enviado tramas a una velocidad de transmisión de 2 Mbps (1701 tramas enviadas) obtenemos un 6.1% de tramas perdidas (1598 tramas recibidas).

Medición de Jitter a 20 kbps:

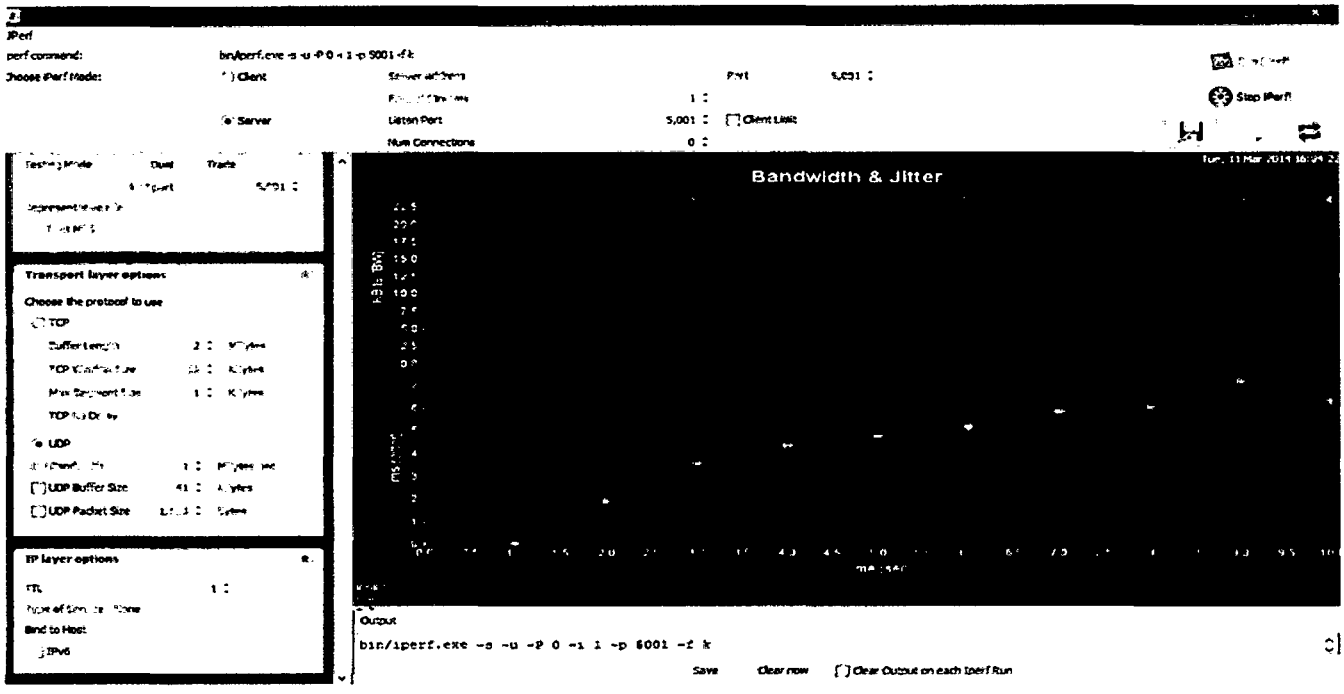


Fig. 4.2.24 Gráfica de Bandwidth y Jitter

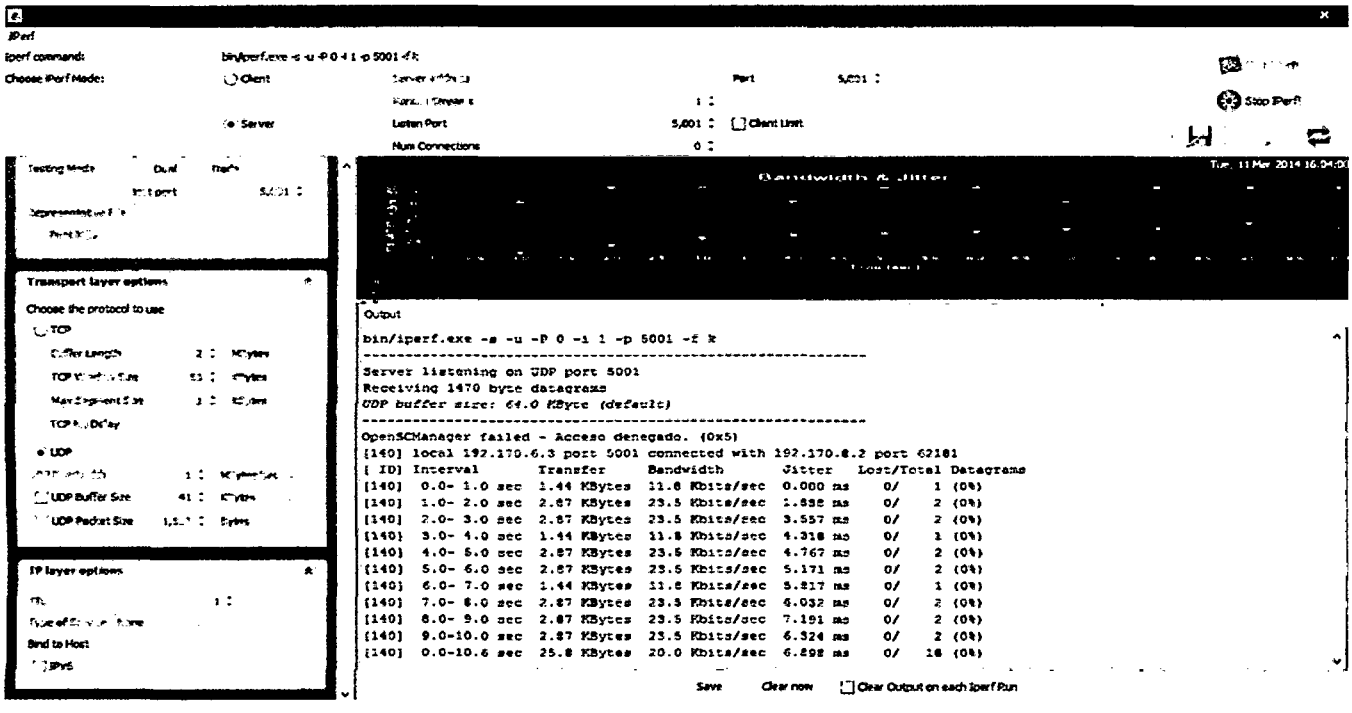


Fig. 4.2.25 Resultados al medir Throughput como servidor

PASO 4: Captura de tráfico con Wireshark.

Capturar tráfico de paquetes en la interfaz s0/0 de R2.

- Captura de paquetes ICMP.

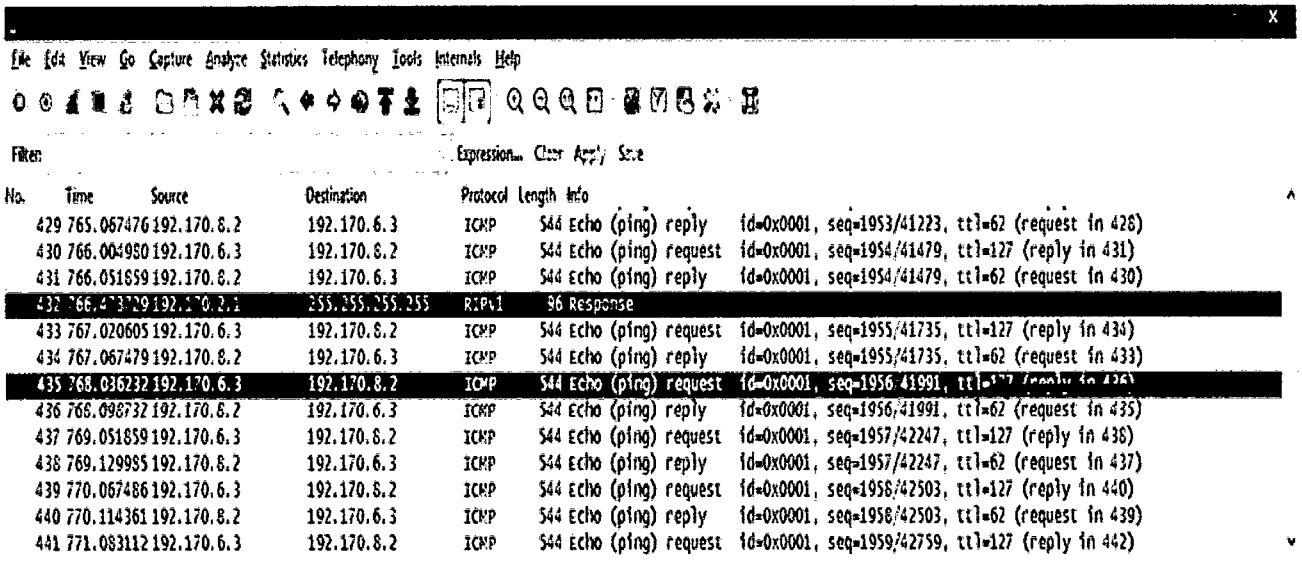


Fig. 4.2.26 Captura de paquetes ICMP con Wireshark

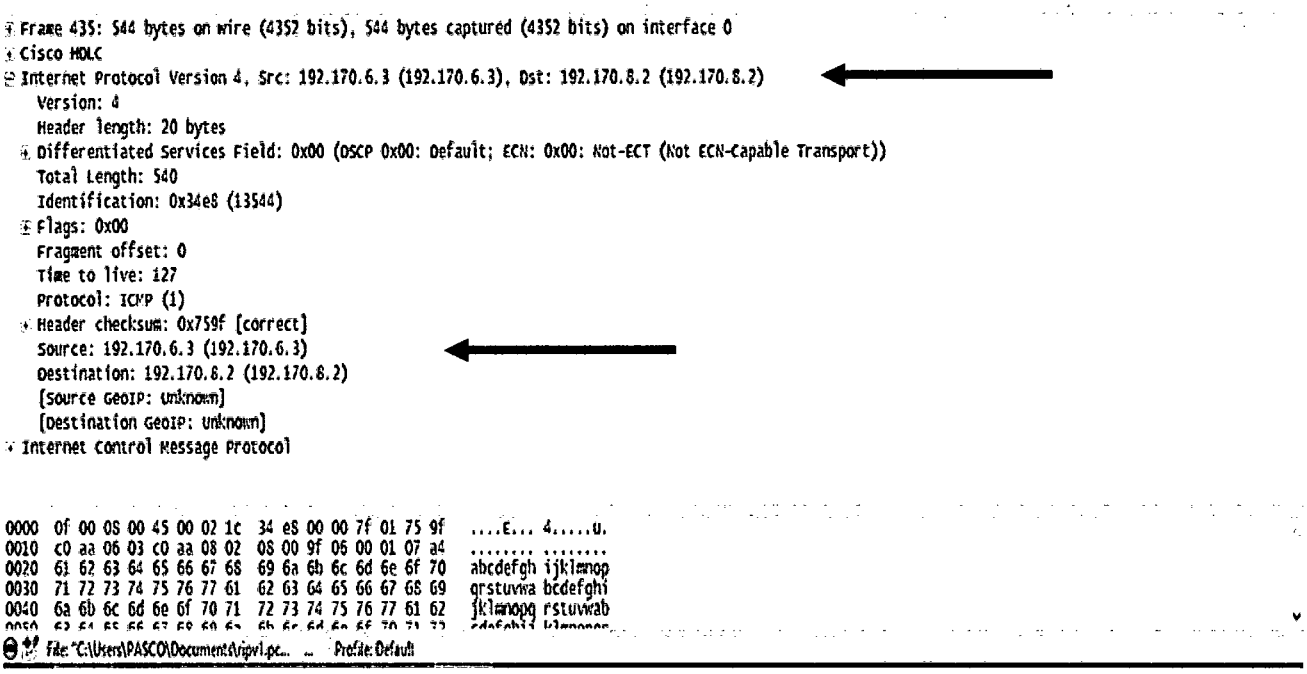


Fig. 4.2.27 Información detallada del paquete ICMP.

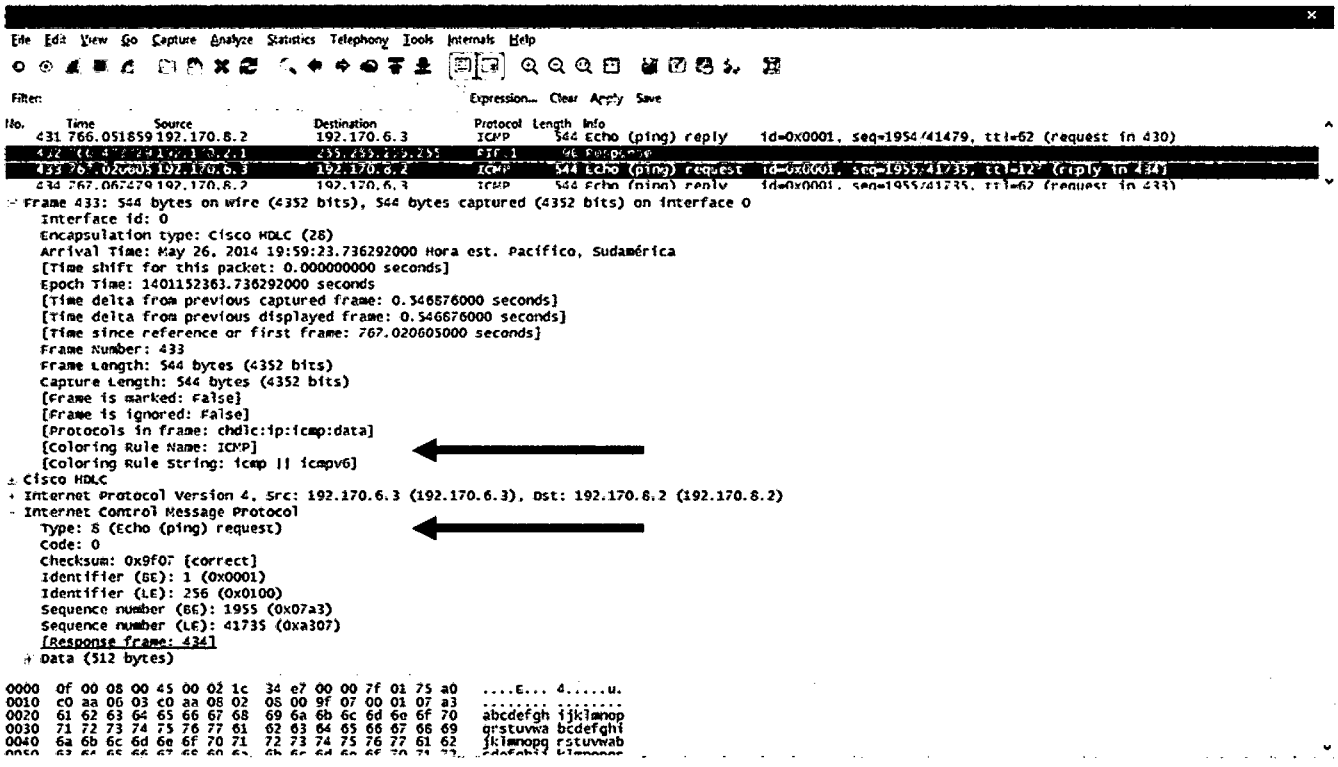


Fig. 4.2.28 Información detallada del paquete ICMP.

- Protocolo de enrutamiento RIPv1:

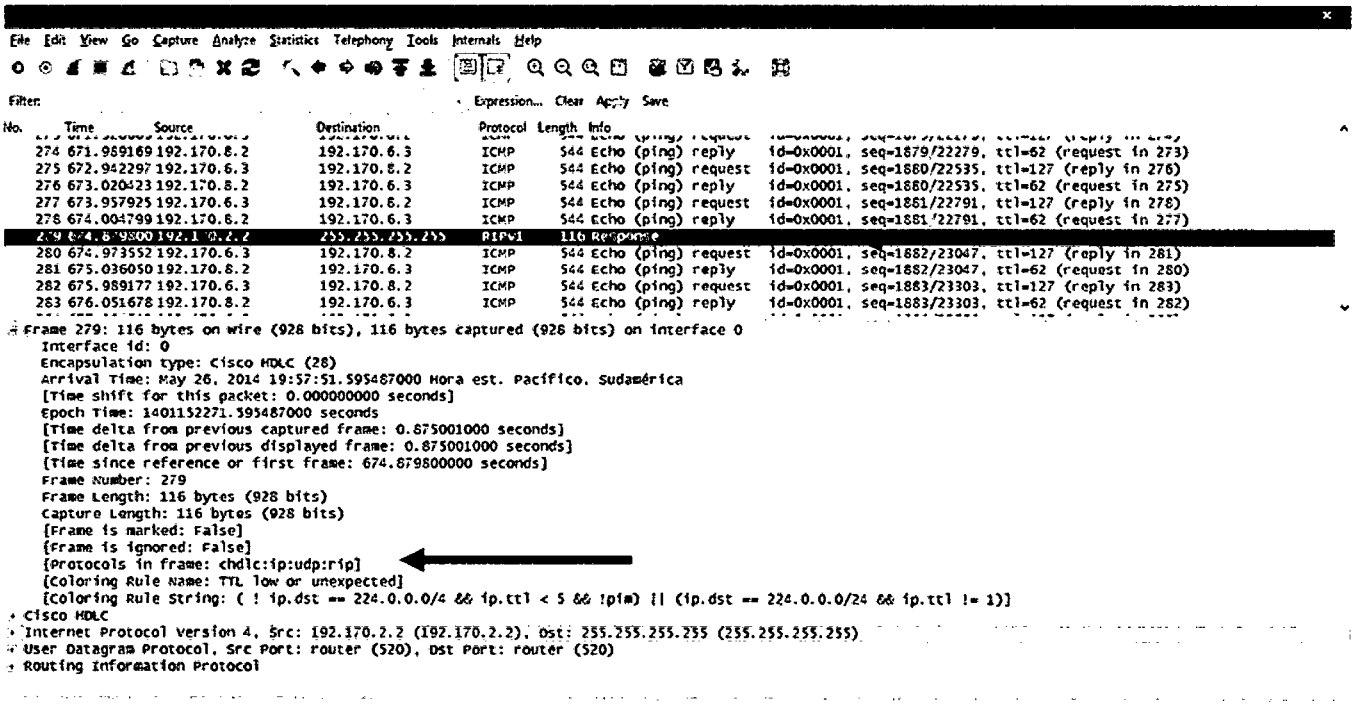


Fig. 4.2.29 Captura del RIPv1 con Wireshark

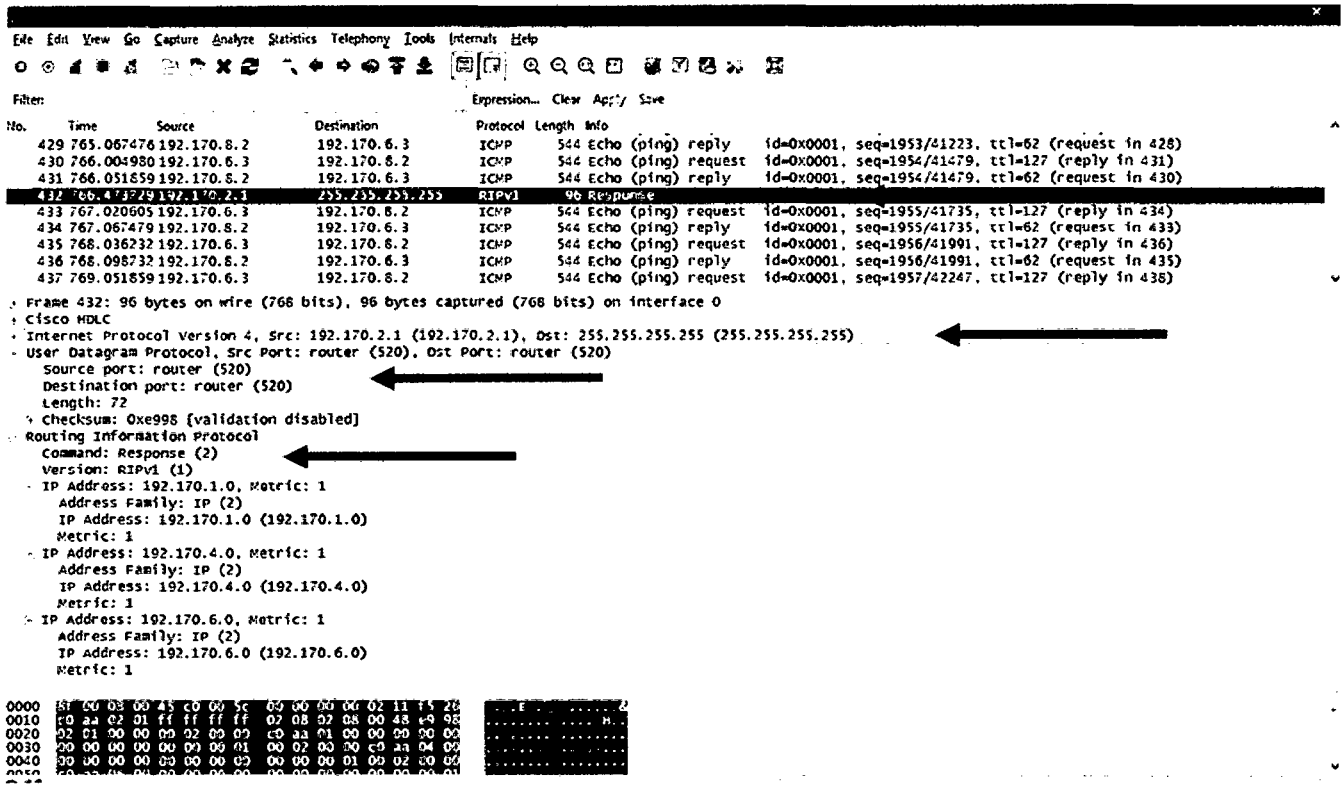


Fig. 4.2.30 Información detallada del protocolo RIPv1

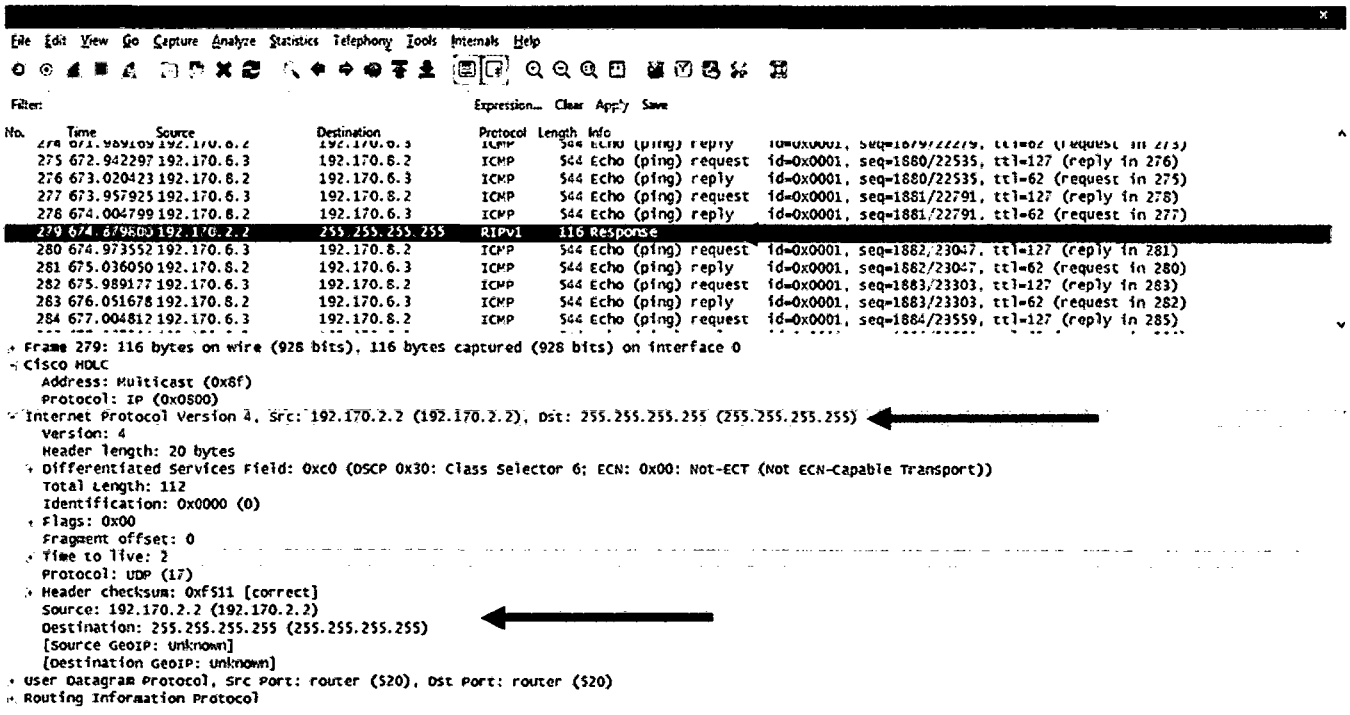


Fig. 4.2.31 Información del protocolo RIPv1

LABORATORIO 4.3: CALCULO DE VLSM Y CONFIGURACION DE ENTRUTAMIENTO DINAMICO CON RIP V2

REVISIÓN TEÓRICA: Para la realización de esta práctica se deberá revisar conceptos de RIP versión 2.

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Determinar la cantidad de subredes necesarias.
- Determinar la cantidad de hosts necesarios para cada subred.
- Diseñar un esquema de direccionamiento adecuado utilizando VLSM.
- Asignar direcciones y pares de máscaras de subred a las interfaces del dispositivo.
- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet.
- Configurar una ruta dinámica con el protocolo de enrutamiento RIPv2 en todos los routers.
- Verificar el enrutamiento RIPv2 con los comandos **show ip route, show ip protocols** y las actualizaciones de enrutamiento con **debug ip rip**.
- Desactive la sumarización automática.
- Examinar las tablas de enrutamiento.
- Probar la conectividad de la red.
- Análisis de tráfico de paquetes.

ESCENARIO:

En este laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **172.16.0.0/16** para obtener el direccionamiento IP usando VLSM, teniendo los siguientes requisitos:

LAN 1 de R5: 118 direcciones IP de host.
LAN 2 de R3: 86 direcciones IP de host.
LAN 3 de R1: 50 direcciones IP de host.
LAN 4 de R1: 24 direcciones IP de host.

Considerando también las redes que hay entre router y router (enlaces WAN).

Luego realice las configuraciones básicas en los routers y configure el enrutamiento dinámico para que se realice la comunicación de extremo a extremo entre los hosts de la red. Después de completar la configuración pruebe la conectividad entre los dispositivos de la red y finalmente analizará el tráfico de paquetes en dicha topología.

DIAGRAMA DE TOPOLOGIA:

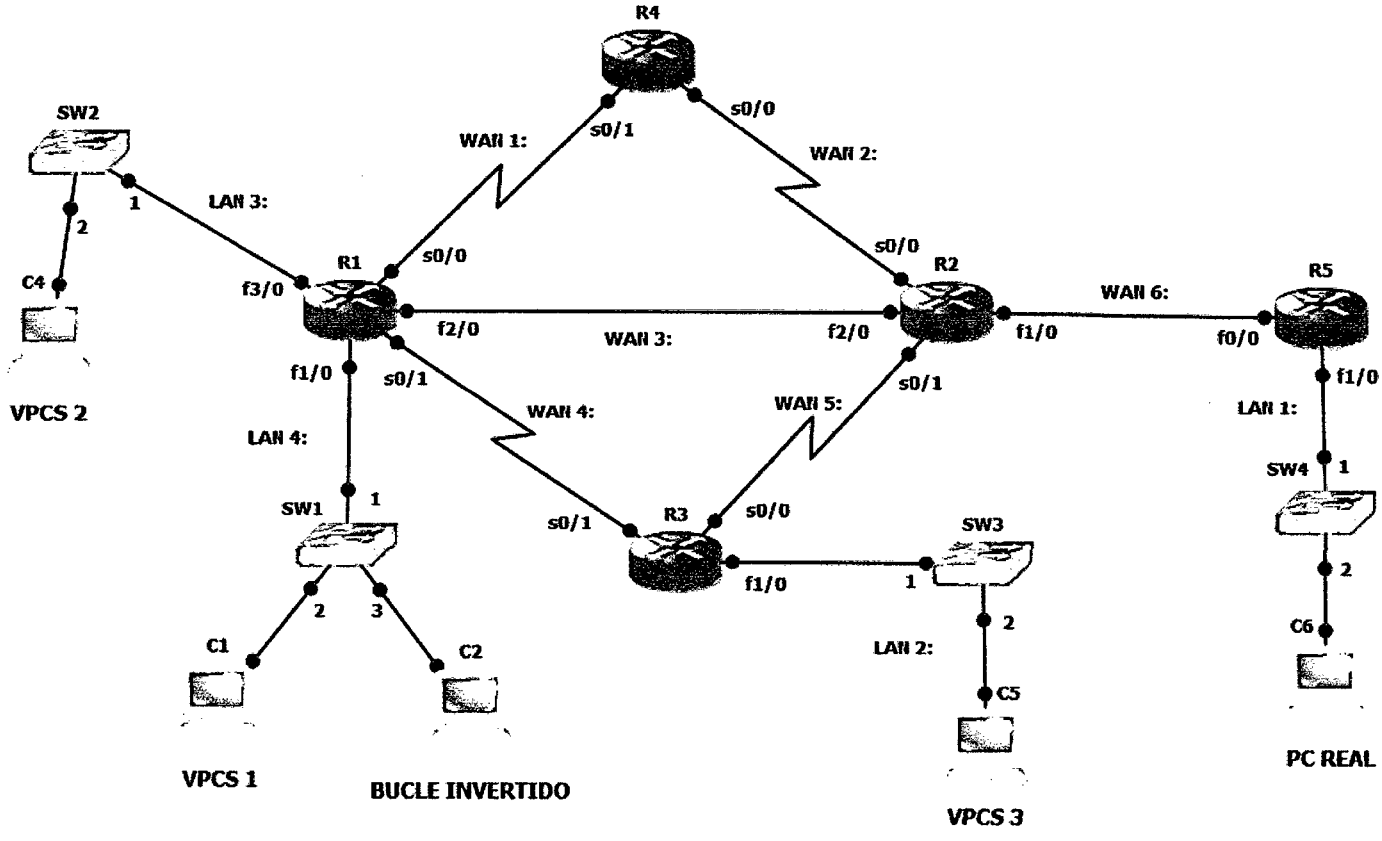


Fig. 4.3.1 Red Virtual en GNS3

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN:

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s0/0	172.16.1.97	255.255.255.252	No aplicable
	s0/1	172.16.1.109	255.255.255.252	No aplicable
	f1/0	172.16.1.65	255.255.255.224	No aplicable
	f2/0	172.16.1.105	255.255.255.252	No aplicable
	f3/0	172.16.1.1	255.255.255.192	No aplicable
R2	s0/0	172.16.1.101	255.255.255.252	No aplicable
	s0/1	172.16.1.113	255.255.255.252	No aplicable
	f1/0	172.16.1.117	255.255.255.252	No aplicable
	f2/0	172.16.1.106	255.255.255.252	No aplicable
R3	s0/0	172.16.1.114	255.255.255.252	No aplicable
	s0/1	172.16.1.110	255.255.255.252	No aplicable
	f1/0	172.16.0.129	255.255.255.128	No aplicable
R4	s0/0	172.16.1.102	255.255.255.252	No aplicable
	s0/1	172.16.1.98	255.255.255.252	No aplicable
R5	g0/0	172.16.1.118	255.255.255.252	No aplicable
	g0/1	172.16.0.1	255.255.255.128	No aplicable
C1	VPCS	172.16.1.66	255.255.255.224	172.16.1.65
C4	VPCS	172.16.1.2	255.255.255.192	172.16.1.1
C5	VPCS	172.16.0.130	255.255.255.128	172.16.0.129
C2	BUCLE INVERTIDO	172.16.1.67	255.255.255.224	172.16.1.65
PC REAL	NIC	172.16.0.2	255.255.255.128	172.16.0.1

Tabla 4.3.1 Direccionamiento IP para las Redes

TAREA 1: MONTAR LA RED EN GNS3

Montar y conectar la red igual a la del Diagrama de topología.

TAREA 2: EXAMINAR LOS REQUISITOS DE LA RED

Examine los requisitos de la red y responda las siguientes preguntas. Tenga presente que se necesitarán direcciones IP para cada una de las interfaces LAN.

1. ¿Cuántas subredes se necesitan? _____

2. ¿Cuál es la cantidad máxima de direcciones IP que se necesitan para una única subred?

_____

3. ¿Cuántas direcciones IP se necesitan para la LAN de R5? _____

4. ¿Cuántas direcciones IP se necesitan para cada una de las LAN de R1? _____

5. ¿Cuántas direcciones IP se necesitan para cada uno de estos enlaces WAN entre routers? ____

6. ¿Cuál es la cantidad total de direcciones IP que se necesitan? _____

7. ¿Cuál es la subred de menor tamaño que puede utilizarse? _____

8. ¿Cuál es el número máximo de direcciones IP que se puede asignar en una subred de este tamaño? _____

9. ¿Cuál es el número total de direcciones IP que están disponibles en la red 172.16.0.0/16? _____

10. ¿Se pueden lograr los requerimientos de direccionamiento de red utilizando la red

172.16.0.0/16? _____

TAREA 3: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

Una vez iniciado el equipo aparecerá el siguiente prompt:

Router>

Ingrese al modo privilegiado

Router>enable

Aparece el siguiente prompt

Router#

PASO 1: Establezca la configuración global del nombre de host.

En el modo exec privilegiado, ingrese al modo de configuración global:

Router# **configure terminal**

Ingrese el siguiente comando para configurar el nombre del router:

Router(config)#**hostname XXXXXX** (Escribir nombre deseado)

PASO 2: Configure un mensaje para que se muestre al ingresar al router.

Router(config)#**banner motd %** Solo acceso a personal autorizado **%** (Puede escribir cualquier mensaje)

El símbolo % indica el inicio y final del mensaje

PASO 3: Configure las contraseñas de consola, enable secret y VTY.

Seguir los siguientes pasos:

Router(config)# **line console 0**

Router(config-line)# **password XXXXX**

Router(config-line)# **login**

Router(config-line)# **exit**

Router(config)# **enable secret XXXXX**

Router(config)# **line vty 0 4**

Router(config-line)# **password XXXXX**

Router(config-line)# **login**

Router(config-line)# **exit**

PASO 4: Desactive la búsqueda DNS.

Router(config)# **no ip-domain lookup**

Si escribes algo que no sea un comando de Cisco IOS o cometes un error, el router asume que ha escrito un nombre de dominio y trata de resolver lo que usted escribe, realizando una búsqueda de DNS.

PASO 5: Sincronice los mensajes no solicitados y el resultado de la depuración con el resultado solicitado y los indicadores para las líneas de consola y de terminal virtual.

Router(config)# **line console 0**

Router(config)# **logging synchronous**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **logging synchronous**

Router(config)# **exit**

PASO 6: Configure un tiempo de espera EXEC de 10 minutos.

Router(config)# **line console 0**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

PASO 7: Guardar la configuración.

Router(config)# **copy running-config startup-config**

TAREA 4: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET.

Aplique Los siguientes comandos:

R1:

Configuración para una interface serial DCE:

R1(config)# **interface serial 0/0**

R1(config-if)# **description conexion a R4**

R1(config-if)# **ip address 172.16.1.97 255.255.255.252**

R1(config-if)#**clock rate 64000**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

Configuración para una interface fasEthernet:

R1(config)# **interface fasEthernet 1/0**

R1(config-if)# **description conexion a LAN 4**

R1(config-if)# **ip address 172.16.1.65 255.255.255.224**

R1(config-if)# **no shutdown**

R1(config-if)# **end**

R1(config)# **interface fasEthernet 2/0**

R1(config-if)# **description conexion a R2**

R1(config-if)# **ip address 172.1.1.105 255.255.255.252**

R1(config-if)# **no shutdown**

R1(config-if)# **end**

R1(config)# **interface fasEthernet 3/0**

R1(config-if)# **description conexion a LAN 3**

R1(config-if)# **ip address 172.16.1.1 255.255.255.192**

R1(config-if)# **no shutdown**

R1(config-if)# **end**

R4:

Configuración para una interface serial DTE:

R4(config)# **interface serial 0/0**

R4(config-if)# **description conexion a R2**

R4(config-if)# **ip address 172.16.1.102 255.255.255.252**

R4(config-if)# **no shutdown**

R4(config-if)# **exit**

NOTA: Seguir los mismos pasos para la configuración de las interfaces de los demás routers.

TAREA 5: CONFIGURAR LAS RUTAS DINÁMICAS MEDIANTE EL PROTOCOLO DE ENRRUTAMIENTO RIPv2.

PASO 1: Habilite un enrutamiento dinámico.
Para habilitar un protocolo de enrutamiento dinámico, ingrese al modo de configuración global y utilice el comando **router**.

Ingrese **router ?** en el indicador de configuración global para visualizar una lista de los protocolos de enrutamiento disponibles en el router.

Para habilitar RIPv2, ingrese el comando **router rip** en el modo de configuración global.

Configuracion de R1:

R1#**configure terminal**

R1(config)#**router rip**

R1(config-router)#

PASO 2: Ingrese direcciones de red, utilice el comando version 2 para habilitar RIP versión 2 en cada uno de los routers.

Una vez que se encuentre en el modo de configuración de enrutamiento, ingrese la dirección de red con clase para cada red conectada directamente por medio del comando **network**.

R1(config-router)#**network 172.16.1.96**
R1(config-router)#**network 172.16.1.108**

R1(config-router)#**network 172.16.1.104**
R1(config-router)#**network 172.16.1.0**
R1(config-router)#**network 172.16.1.64**
R1(config-router)# **version 2**
R1(config-router)#**no auto-summary**
R1(config-router)#**passive-interface fastethernet 1/0**
R1(config-router)#**passive-interface fastethernet 3/0**

R1(config-router)#

Comando **network**:

- Habilita a RIP en todas las interfaces que pertenezcan a esta red. Ahora estas interfaces enviarán y recibirán actualizaciones RIP.
- Notifica esta red en actualizaciones de enrutamiento RIP que se envían a otros routers cada 30 segundos.

El comando no auto-summary se utiliza para desactivar el resumen automático en RIPv2. Deshabilite el resumen automático en todos los routers. Los routers ya no resumirán las rutas en los bordes de redes principales.
Enviar actualizaciones desde la interfaz desperdicia ancho de banda y recursos de procesamiento de todos los dispositivos de la LAN. Además, notificar actualizaciones en una red de broadcast es un riesgo para la seguridad. Las actualizaciones RIP pueden interceptarse con software analizador de protocolos. Las actualizaciones de enrutamiento pueden modificarse y enviarse de regreso al router, dañando la tabla del router con métricas falsas que orientan mal el tráfico. El comando passive-interface fastethernet 1/0 se utiliza para deshabilitar el envío de actualizaciones RIPv2 a la interfaz.
Al finalizar la configuración RIPv2, regrese al modo EXEC privilegiado y guarde la configuración actual para la NVRAM.

R1(config-router)#**end**
%SYS-5-CONFIG_I: Configured from console by console
R1#**copy run start**

Los mensajes RIPv2 incluyen la máscara de subred en un campo en las actualizaciones de enrutamiento. Esto permite que las subredes y sus máscaras se incluyan en las actualizaciones de enrutamiento. No obstante, por defecto, RIPv2 resume las redes en los bordes de redes principales, como RIPv1, excepto que la máscara de subred está incluida en la actualización.

PASO 3: Configure RIPv2 en el router R3 por medio de los comandos router rip, network y versión 2.

R3(config)#**router rip**
R3(config-router)#**network 172.16.1.108**
R3(config-router)#**network 172.16.1.112**

R3(config-router)#**network 172.16.0.128**
R3(config-router)# **version 2**
R3(config-router)#**no auto-summary**
R1(config-router)#**passive-interface fastethernet 1/0**
R3(config-router)#**end**
%SYS-5-CONFIG_I: Configured from console by console
R2#**copy run start**

Al finalizar la configuración RIP, regrese al modo EXEC privilegiado y guarde la configuración actual para la NVRAM.

NOTA: Seguir los mismos pasos para la configuración de los routers R2, R4 y R5.

TAREA 6: CONFIGURAR LOS EQUIPOS DE HOST.

Configurar las direcciones IP y gateways por defecto como se indican en la tabla de direccionamiento de las interfaces Ethernet de C1, C2 (VPCS) y PC REAL.

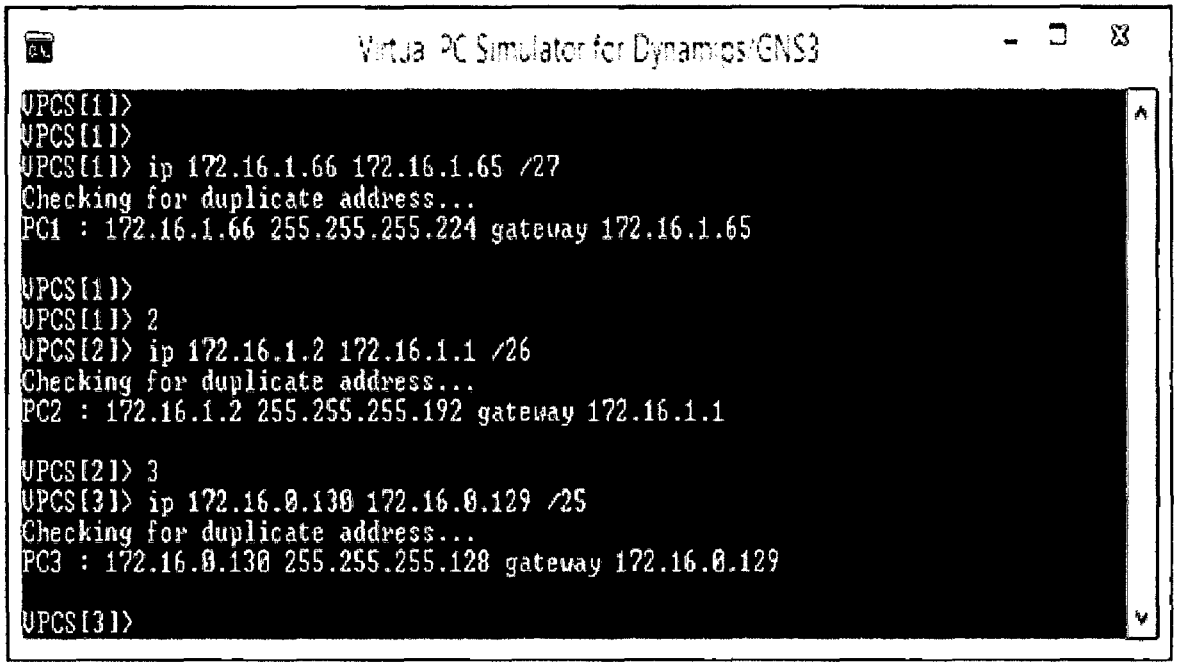


Fig. 4.3.2 Configuración de la Direccion IP de las VPCS

TAREA 7: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

PASO 1: Verificar el direccionamiento IP y las interfaces.

R1# **show ip interface brief**

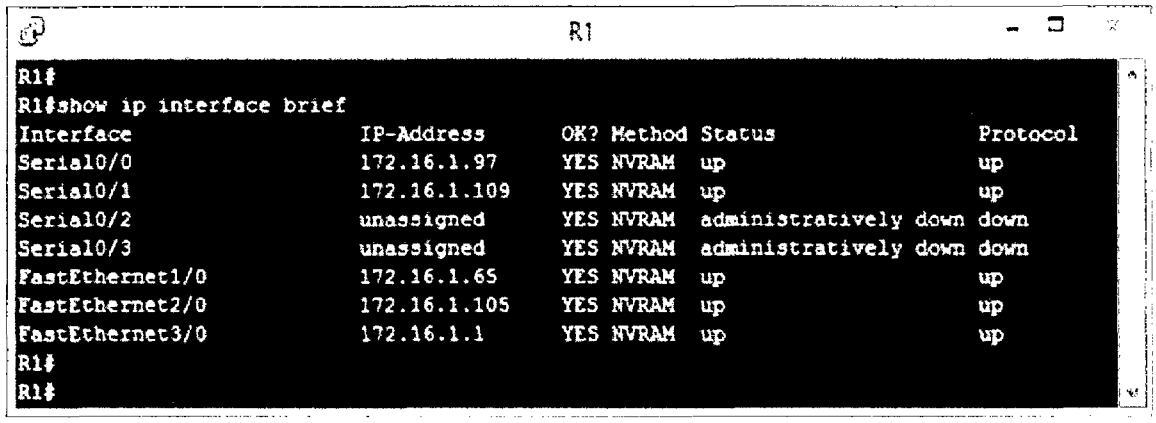


Fig. 4.3.3 Tabla ip de Interfaces Activas de R1.

R2# **show ip interface brief**

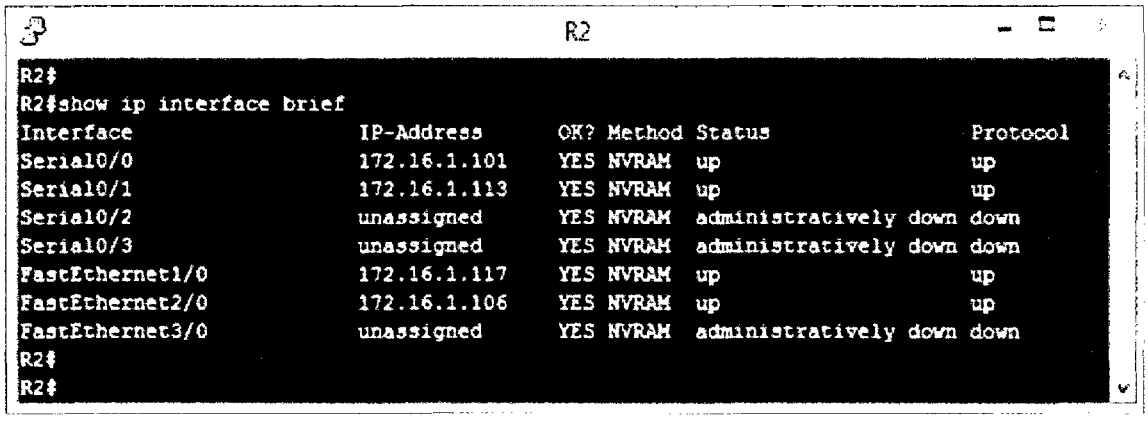


Fig. 4.3.4 Tabla ip de Interfaces Activas de R2.

NOTA: Verificar que las interfaces de los demás routers tengan la adecuada dirección IP y estén activas.

PASO 2: Verificar la configuración de los router. Use los comandos **show ip route** para verificar el contenido de la tabla de enrutamiento.

R1# **show ip route**

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 10 subnets, 4 masks
R       172.16.0.128/25 [120/1] via 172.16.1.110, 00:00:07, Serial0/1
R       172.16.0.0/25 [120/2] via 172.16.1.106, 00:00:16, FastEthernet2/0
C       172.16.1.0/26 is directly connected, FastEthernet3/0
R       172.16.1.116/30 [120/1] via 172.16.1.106, 00:00:16, FastEthernet2/0
R       172.16.1.112/30 [120/1] via 172.16.1.110, 00:00:07, Serial0/1
                        [120/1] via 172.16.1.106, 00:00:16, FastEthernet2/0
C       172.16.1.108/30 is directly connected, Serial0/1
C       172.16.1.104/30 is directly connected, FastEthernet2/0
R       172.16.1.100/30 [120/1] via 172.16.1.106, 00:00:18, FastEthernet2/0
                        [120/1] via 172.16.1.98, 00:00:35, Serial0/0
C       172.16.1.96/30 is directly connected, Serial0/0
C       172.16.1.64/27 is directly connected, FastEthernet1/0
R1#
```

Fig. 4.3.5 Tabla de enrutamiento de R1

R2# **show ip route**

```
R2#
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 10 subnets, 4 masks
R       172.16.0.128/25 [120/1] via 172.16.1.114, 00:00:10, Serial0/1
R       172.16.0.0/25 [120/1] via 172.16.1.118, 00:00:06, FastEthernet1/0
R       172.16.1.0/26 [120/1] via 172.16.1.105, 00:00:01, FastEthernet2/0
C       172.16.1.116/30 is directly connected, FastEthernet1/0
C       172.16.1.112/30 is directly connected, Serial0/1
R       172.16.1.108/30 [120/1] via 172.16.1.114, 00:00:10, Serial0/1
                        [120/1] via 172.16.1.105, 00:00:01, FastEthernet2/0
C       172.16.1.104/30 is directly connected, FastEthernet2/0
C       172.16.1.100/30 is directly connected, Serial0/0
R       172.16.1.96/30 [120/1] via 172.16.1.105, 00:00:03, FastEthernet2/0
                       [120/1] via 172.16.1.102, 00:00:13, Serial0/0
R       172.16.1.64/27 [120/1] via 172.16.1.105, 00:00:03, FastEthernet2/0
R2#
```

Fig. 4.3.6 Tabla de Enrutamiento de R2

PASO 3: Utilice el comando ***show ip protocols*** para visualizar la información acerca de los procesos de enrutamiento.

El comando **show ip protocols** se puede utilizar para visualizar información acerca de los procesos de enrutamiento que se producen en el router. Se puede utilizar este resultado para verificar los parámetros RIPv2 para confirmar que:

- El uso del enrutamiento RIPv2 está configurado.
- Las interfaces correctas envían y reciben las actualizaciones RIPv2.
- El router notifica las redes correctas.
- Los vecinos RIPv2 están enviando actualizaciones.

Fig. 4.3.7 Procesos de Enrutamiento

R1 sí está configurado con RIPv2. R1 está enviando y recibiendo actualizaciones RIP en FastEthernet1/0, FastEthernet2/0, FastEthernet3/0, Serial0/0 y serial0/1. R1 está notificando las redes 172.16.1.96, 172.16.1.104, 172.16.1.108, 172.16.1.64 y 172.16.1.0. R1 tiene una fuente de información de enrutamiento. R2, R3, R4 y R5 le están enviando actualizaciones a R1.

PASO 4: Utilice el comando ***debug ip rip*** para visualizar los mensajes RIP que se envían y reciben.

Las actualizaciones rip se envían cada 30 segundos, por lo que deberá esperar para visualizar la información de depuración.

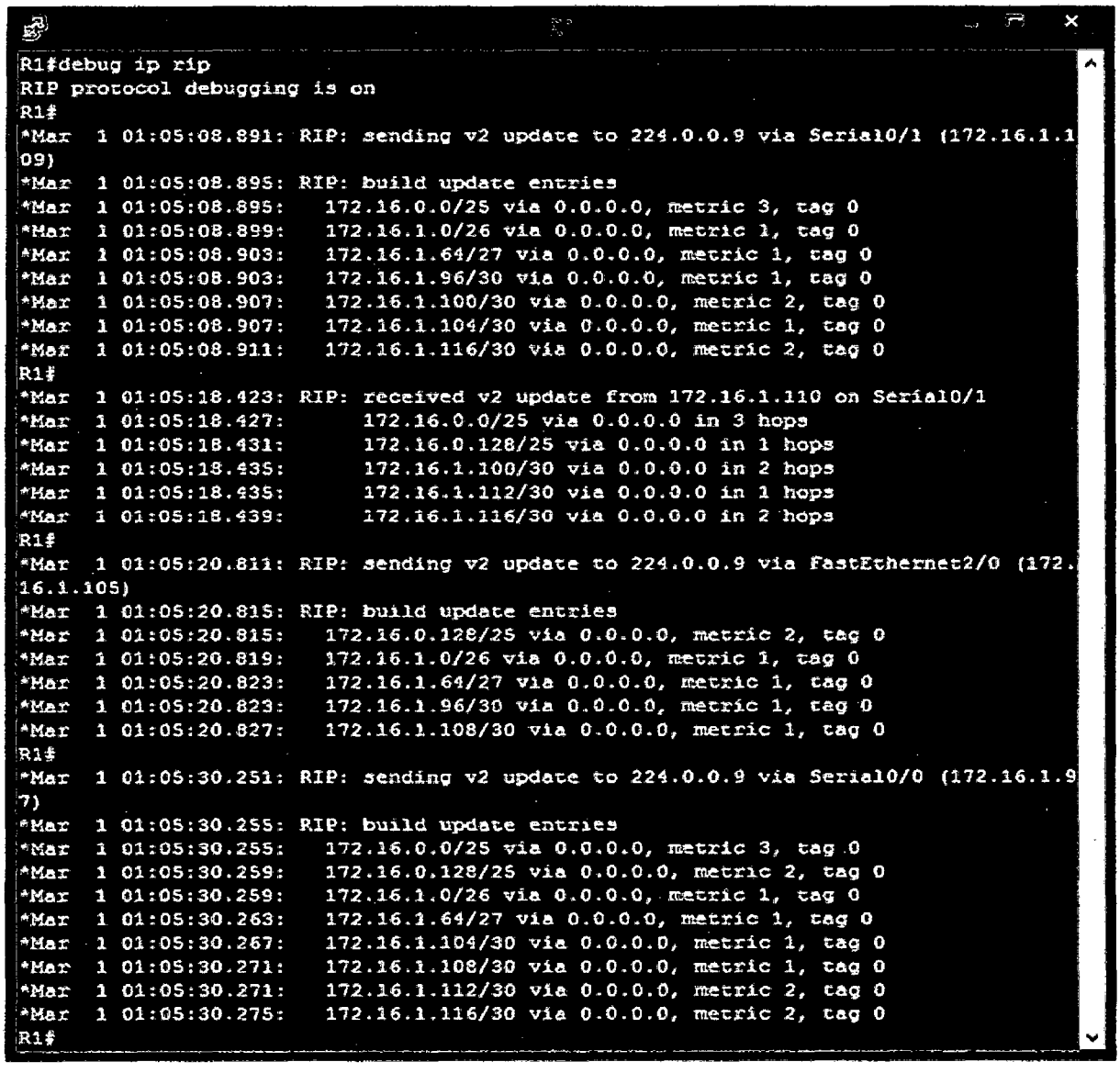


Fig. 4.3.8 Mensajes del Protocolo RIP

El resultado de la depuración muestra que R1 recibe una actualización de los otros routers. Observe cómo esta actualización incluye todas las redes que R1 aún no tiene en su tabla de enrutamiento. Debido a que las interfaces FastEthernet3/0 FastEthernet1/0 pertenecen a la red 172.16.1.0 y 172.16.1.64 configuradas en RIPv2, R1 crea una actualización para enviar a esas interfaces. La actualización incluye todas las redes conocidas para R1, excepto las redes de las interfaces, lo mismo ocurre para las otras interfaces. Por último, R1 crea una actualización para enviar a los demás routers. Debido a esto, R1 incluye en la actualización las redes 172.16.1.0, 172.16.1.96, 172.16.1.108, 172.16.1.64 y 172.16.1.104.

Para detener el resultado de la depuración configure el comando ***undebug all*** en el router.

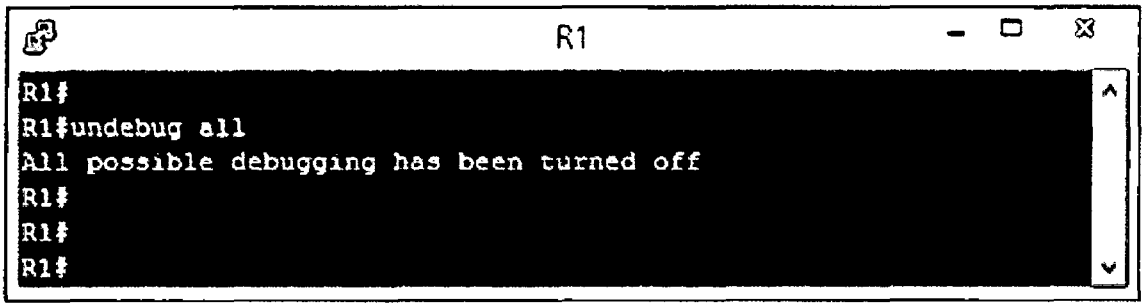


Fig. 4.3.9 Detener Mensajes del Protocolo RIP

PASO 5: Verificar que hay conectividad completa en la red.

Use el comando **ping** para verificar la conectividad.

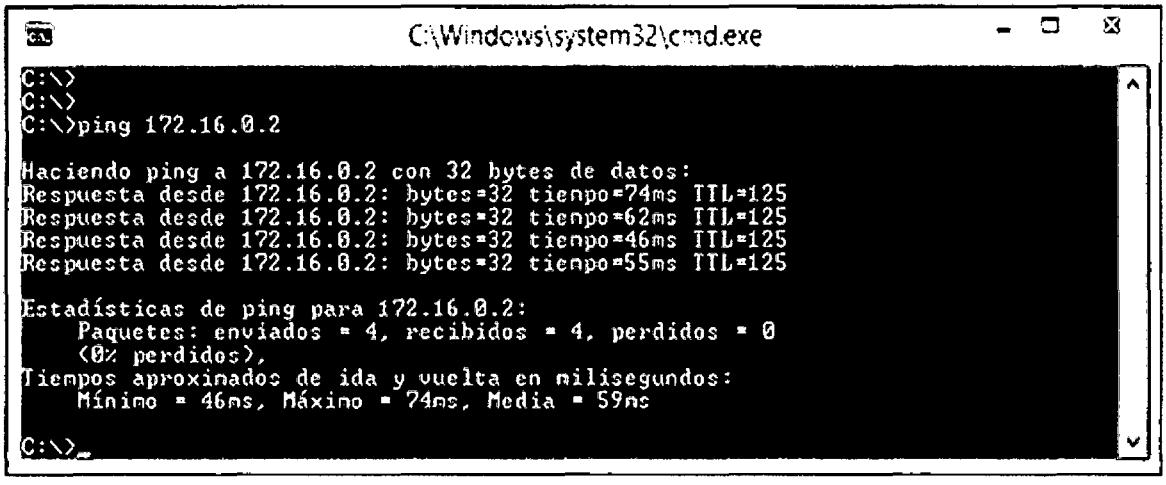


Fig. 4.3.10 Comprobación de conectividad entre C2 y PC Real

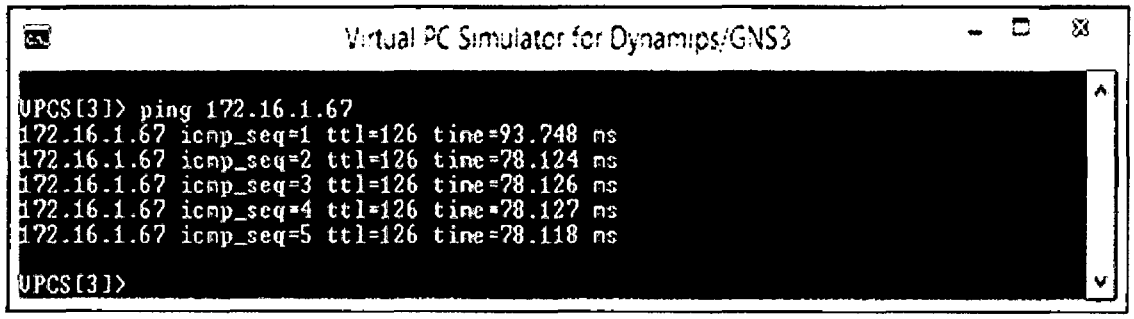


Fig. 4.3.11 Comprobación de conectividad entre C5 y C2

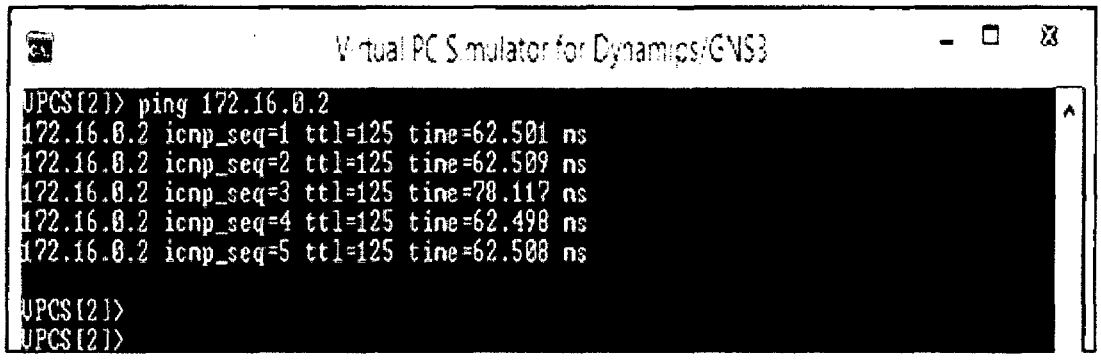


Fig. 4.3.12 Comprobación de conectividad entre C4 y PC Real

PASO 8: ANALIS DEL TRAFICO DE PAQUETES

PASO 1: Medición de la Latencia

Para la medición de la latencia se realizó 10 muestras sucesivas de 100 ping desde el C2 (Bucle invertido) hacia la PC REAL considerando un tamaño de trama de 64, 512 y 1518 bytes como se especifica en el RFC 2544.

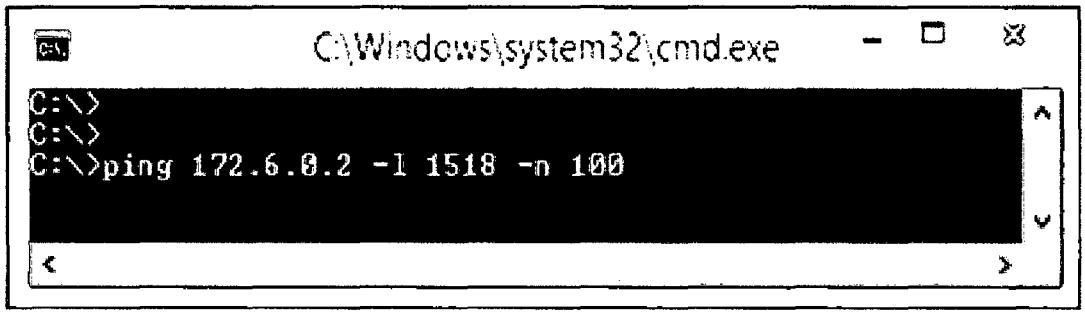


Fig. 4.3.13 Forma de medición de la Latencia

En la Figura 4.3.15 se puede observar el envío de 100 ping con una trama de 1518 hacia la dirección 172.16.0.2.

En las Tablas posteriores se detallan los valores de la Latencia que se ha obtenido una vez realizadas todas las muestras.

LATENCIA											
Tamaño de Trama (bytes)	64										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	47	65	65	47	48	56	65	47	62	47	54.9
Tiempo Máximo (ms)	105	109	133	133	113	118	110	105	122	112	116
Tiempo Promedio (ms)	82	84	92	84	82	82	85	80	85	81	83.7

Tabla 4.3.2 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	512										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	61	47	54	62	61	59	63	61	63	58	58.9
Tiempo Máximo (ms)	116	137	125	292	118	182	207	194	117	204	169.2
Tiempo Promedio (ms)	85	88	85	95	90	91	87	86	85	89	88.1

Tabla 4.3.3 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1518										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	63	63	62	57	63	57	61	64	63	66	61.9
Tiempo Máximo (ms)	205	158	370	137	235	349	243	140	154	125	211.6
Tiempo Promedio (ms)	106	90	110	85	91	107	95	85	89	83	94.1

Tabla 4.3.4 Datos obtenidos para una trama de 1518 bytes.

LATENCIA			
Tamaño de Trama (bytes)	64	512	1518
Tiempo Mínimo (ms)	54.9	58.9	61.9
Tiempo Máximo (ms)	116	169.2	211.6
Tiempo Promedio (ms)	83.7	88.1	94.1

Tabla 4.3.5 Comparación de datos obtenidos de las diferentes tramas.

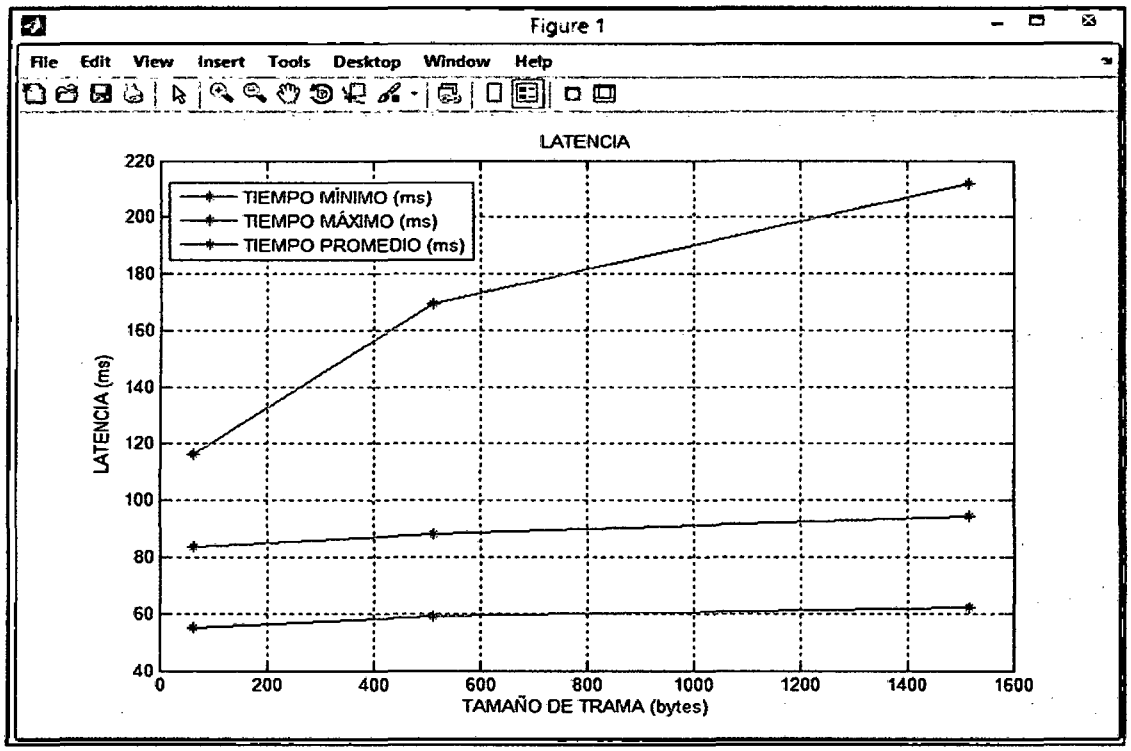


Fig. 4.3.14 Datos representados gráficamente de la variación de la latencia

De acuerdo con los datos obtenidos, se puede observar claramente que los valores mínimo (color azul), máximo (color rojo) y promedio (color verde) de la latencia de la red se incrementan conforme se envía una trama de longitud mayor, en este caso con la trama de 1518 bytes se obtiene una latencia promedio de 64.1 ms a diferencia de una trama de 64 bytes con 57.6 ms.

PASO 2: Medición del Throughput

Para la medición del Throughput y Jitter se envió una cantidad de tramas a velocidades diferentes durante 20 segundos, hasta encontrar la máxima cantidad de tramas recibidas sin que se produzcan perdidas de las mismas en el router y PC REAL. Como se utilizó Jperf el cliente será el encargado de enviar los paquetes y el servidor los recibirá, indicando la cantidad de paquetes que llegaron correctamente considerando un tamaño del paquete UDP de 750, 1125, 1500 y 1470 (default) bytes, tal como se especifica en el RFC 768.

Configuración del Jperf como servidor para medir Throughput:

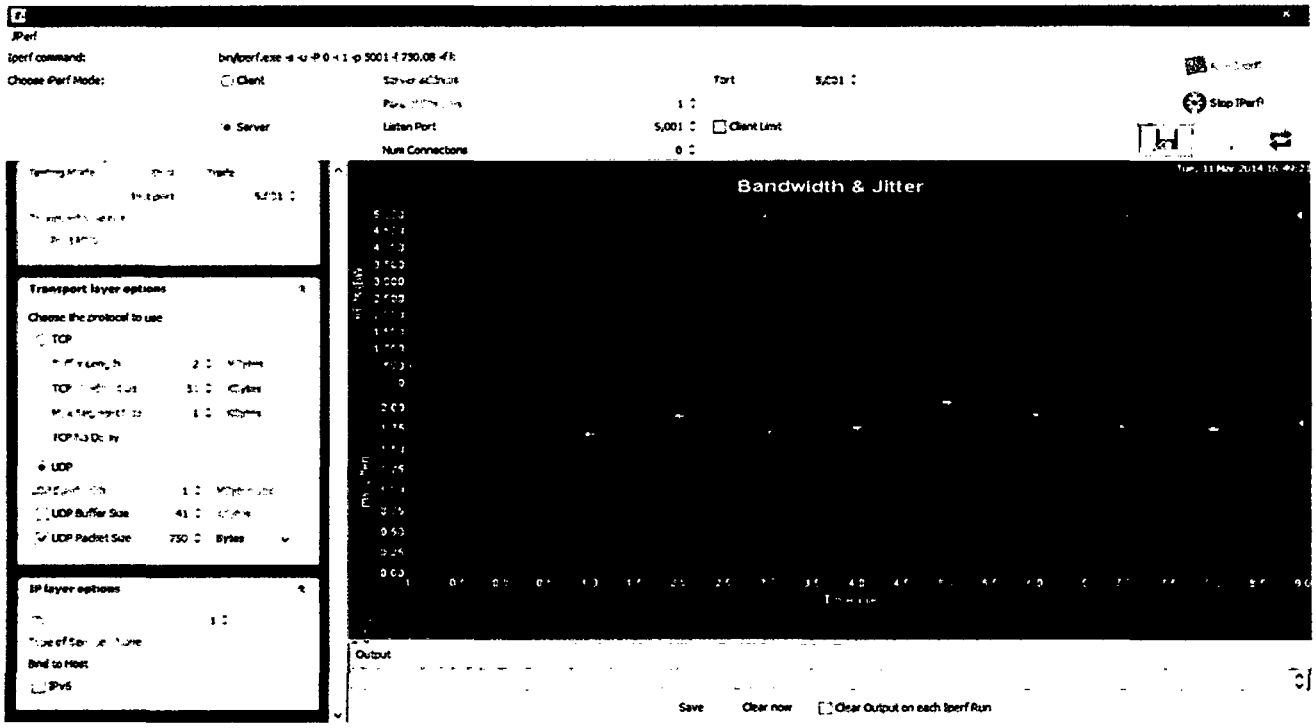


Fig. 4.3.15 Gráfico del Bandwidth y Jitter.

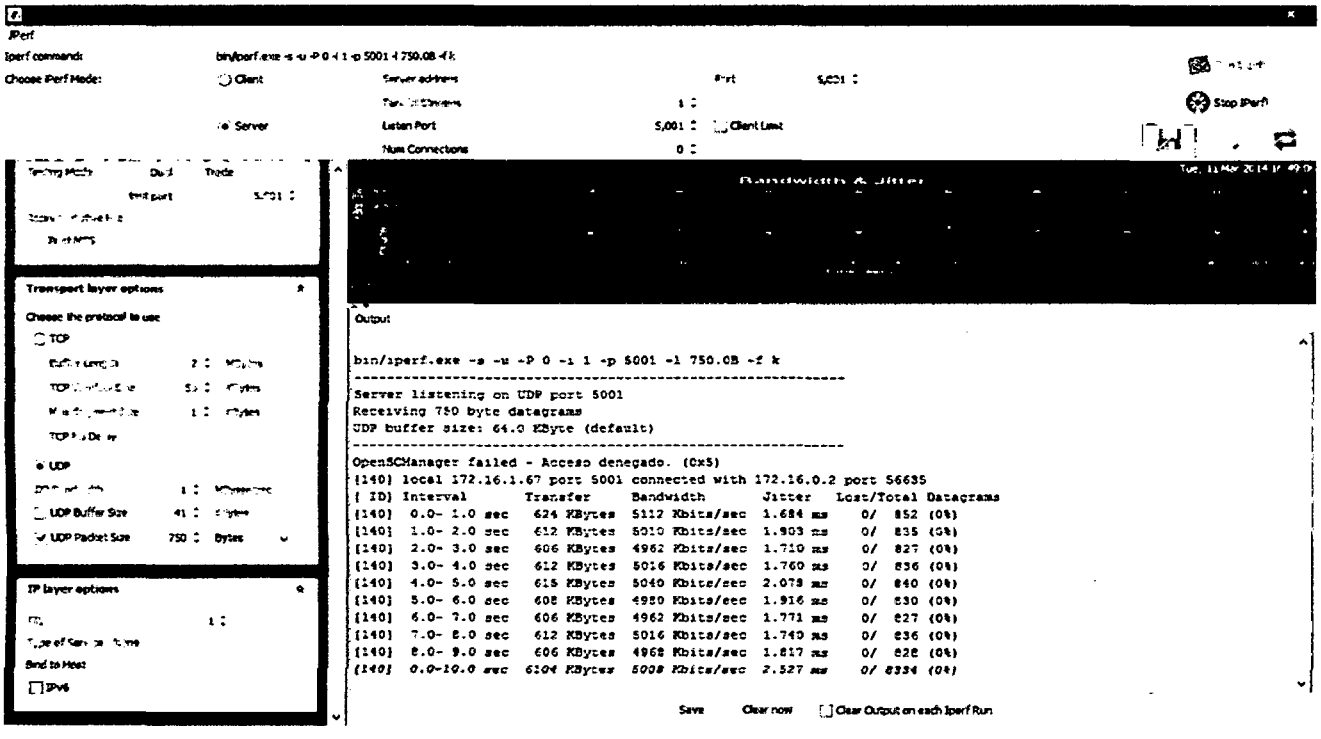


Fig. 4.3.16 Configuración del Jperf como Servidor para medir Jitter.

Configuración del Jperf como cliente para medir Throughput:

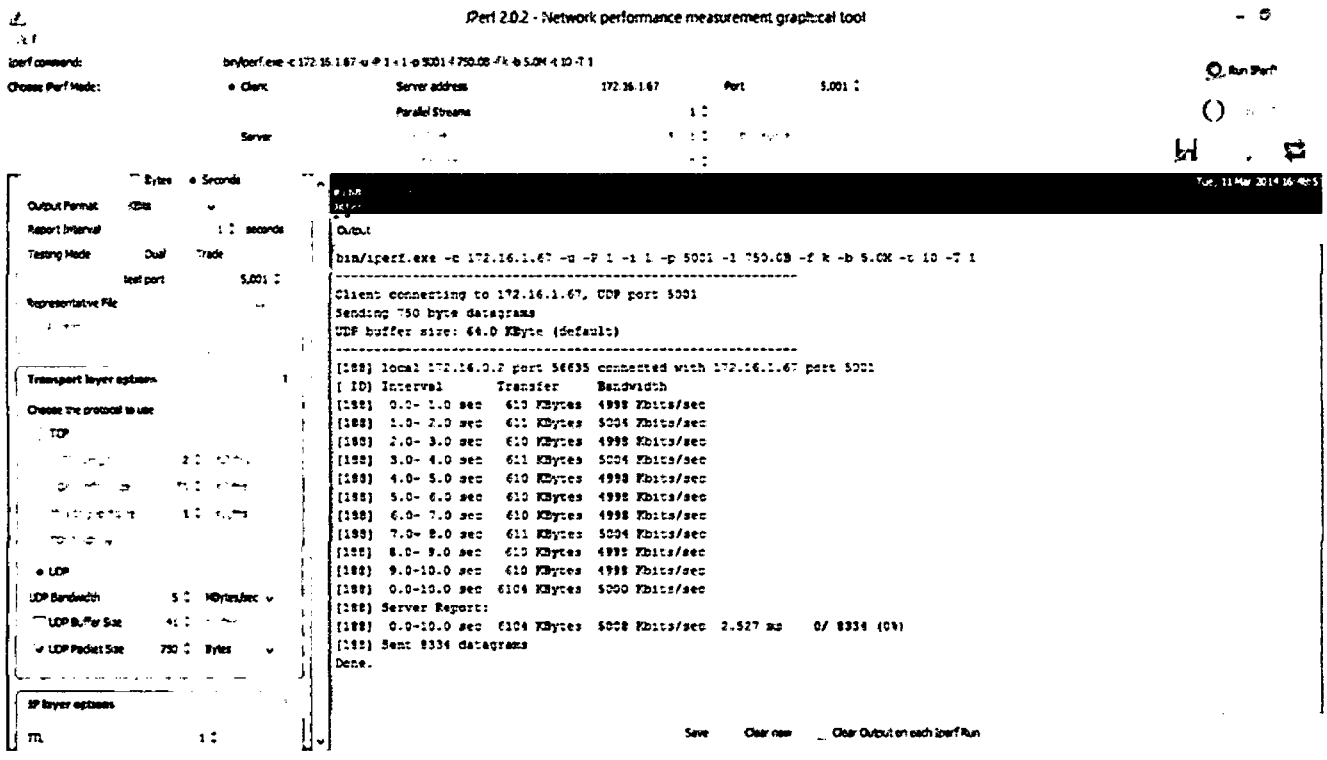


Fig. 4.3.17 Configuración del Jperf como Cliente para medir Throughput.

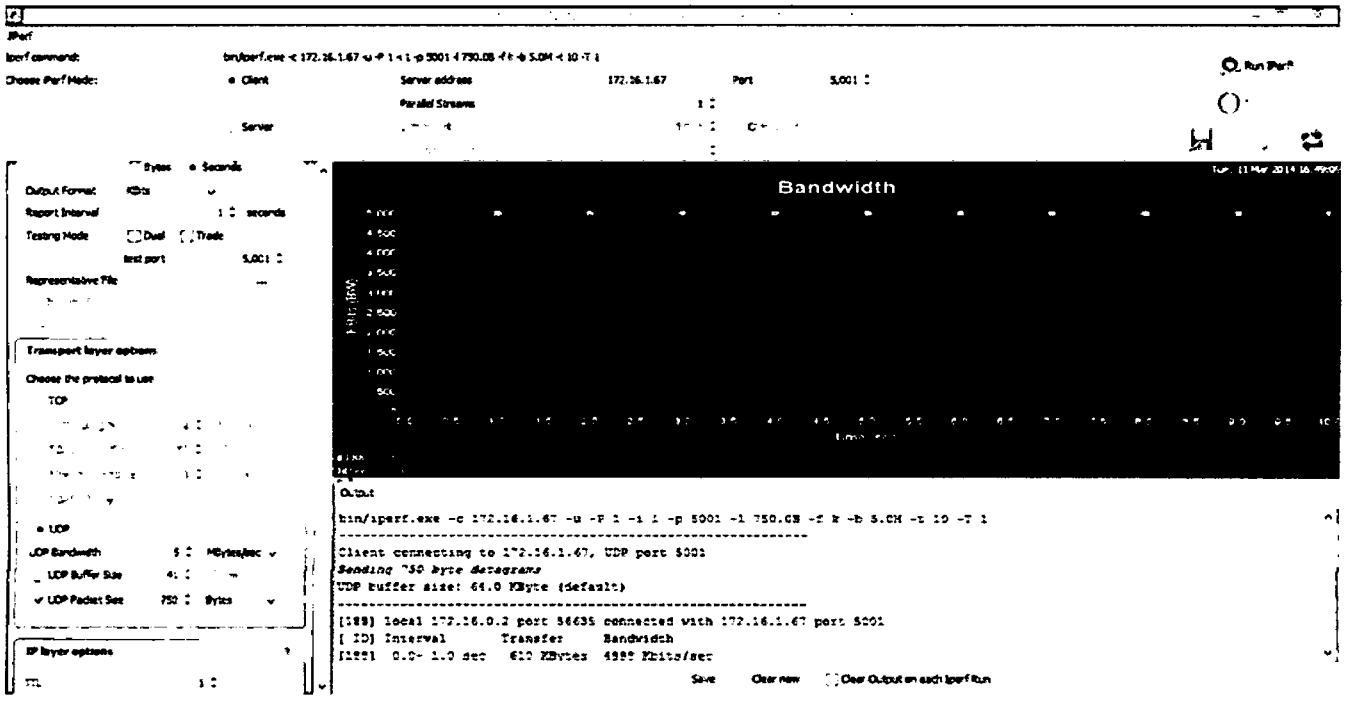


Fig. 4.3.18 Gráfico del Bandwidth en Jperf.

En las siguientes Tablas se detalla los valores del Throughput obtenidos una vez realizada todas las muestras.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**5**	**5**	**5**
Velocidad de Rx (Mbps)	**5**	**5**	**5**
Tramas Transmitidas	**8334**	**5557**	**4168**
Tramas Recibidas	**8334**	**5557**	**4168**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**835**	**556**	**417**

Tabla 4.3.6 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**1**	**4**	**5**	**10**
Velocidad de Rx (Mbps)	**1**	**4**	**5**	**10**
Tramas Transmitidas	**852**	**3400**	**4253**	**8504**
Tramas Recibidas	**852**	**3400**	**4253**	**8504**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**85**	**340**	**426**	**850**

Tabla 4.3.7 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

THROUGHPUT				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**12**	**15**	**20**	**50**
Velocidad de Rx (Mbps)	**10.83**	**7.25**	**5.63**	**4.029**
Tramas Transmitidas	**10205**	**12751**	**17007**	**42447**
Tramas Recibidas	**9455**	**6330**	**5064**	**3512**
Tramas Perdidas	**750 (7.3%)**	**6421 (50%)**	**11943 (70%)**	**38935(92%)**
Tramas Recibidas (pps)	**977**	**1284**	**1741**	**4062**

Tabla 4.3.8 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

En la tabla 4.3.8 observamos que el número de pps aumenta conforme se incrementa la velocidad Tx, pero también aumenta el nueros de paquetes que se pierden en la red sin llegar a su destino, esta topología solo nos soporta una velocidad de Tx de aproximadamente unos 10 Mbps, con velocidades mayores a esta encontramos mucha perdida de paquetes en la red establecida.

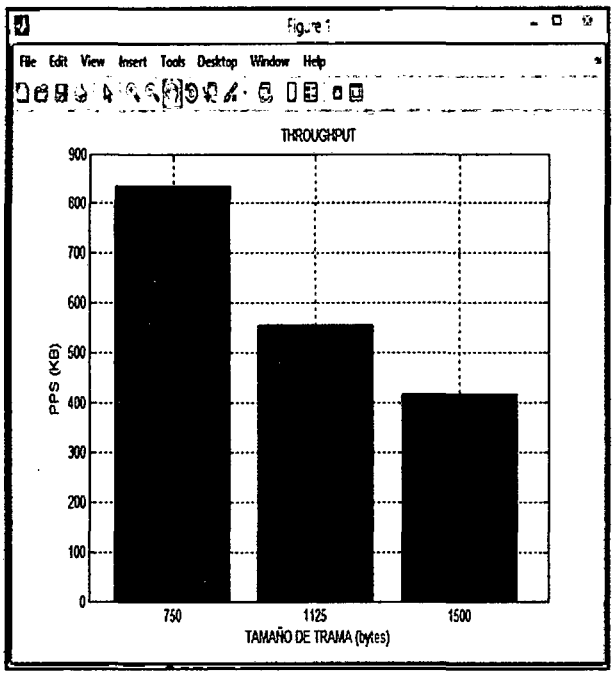


Fig. 4.3.19 PPS vs. Tamaño de Trama

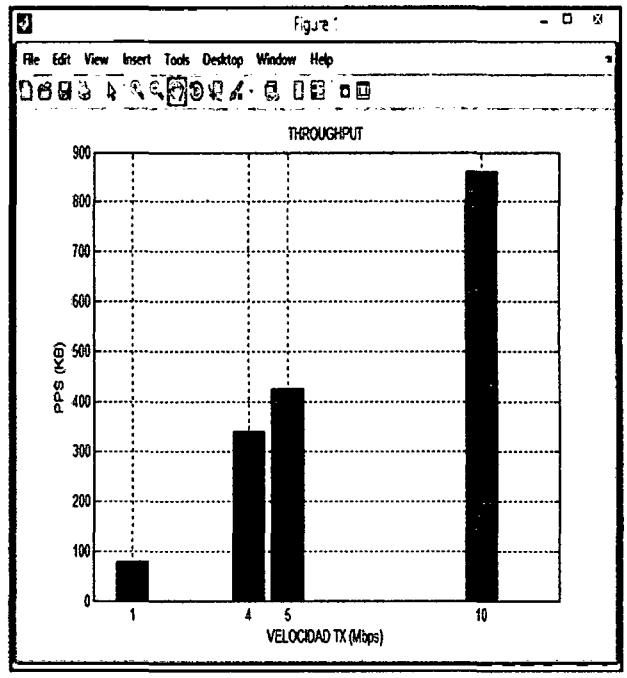


Fig. 4.3.20 PPS vs. Velocidad Tx

En la figura 4.3.18, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 750 bytes, 1125 bytes y 1500 bytes los cuales han utilizado una velocidad de Tx constante de 5 Mbps, en la gráfica se puede observar claramente que al enviar una trama de 750 bytes se envía 835 pps, con una trama de 1125 se envía 556 pps y con una trama de 1500 se envía 417 pps.

Mientras en la figura 4.3.19, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 1470 bytes los cuales han utilizado una velocidad de Tx variada desde 1 Mbps hasta 10 Mbps sin que se produzcan perdidas en el envío, como los datos que se muestran en la tabla 4.3.8 nos indican que enviando tramas a una velocidad mayor de los 12 Mbps se producen pérdidas de paquetes en la red, en la gráfica se observa que a 1 Mbps se envían 85 pps, en cambio a 10 Mbps se obtiene 850 pps.

PASO 3: Medición del Jitter

Para la medición se envió datos UDP de longitud variable a velocidades diferentes de Throughput obtenida anteriormente durante 20 segundos. Como se utilizó anteriormente Jperf el cliente será el encargado de enviar los datos y el servidor los recibirá, indicando los valores de Jitter obtenidos durante la transmisión de los datos.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**5**	**5**	**5**
Velocidad de Rx (Mbps)	**5**	**5**	**5**
Tramas Transmitidas	**8334**	**5557**	**4168**
Tramas Recibidas	**8334**	**5557**	**4168**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**2.527**	**3.089**	**3.777**

Tabla 4.3.9 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**1**	**4**	**5**	**10**
Velocidad de Rx (Mbps)	**1**	**4**	**5**	**10**
Tramas Transmitidas	**852**	**3400**	**4253**	**8504**
Tramas Recibidas	**852**	**3400**	**4253**	**8504**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**4.610**	**3.103**	**2.812**	**1.786**

Tabla 4.3.10 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

JITTER				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**12**	**15**	**20**	**50**
Velocidad de Rx (Mbps)	**10.83**	**7.25**	**5.63**	**4.029**
Tramas Transmitidas	**10205**	**12751**	**17007**	**42447**
Tramas Recibidas	**9455**	**6330**	**5064**	**3512**
Tramas Perdidas	**750 (7.3%)**	**6421 (50%)**	**11943 (70%)**	**38935(92%)**
Jitter (ms)	**1.841**	**2.9**	**3.083**	**3.977**

Tabla 4.3.11 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

En la tabla 4.3.11 apreciamos que la red establecida nos soporta una cantidad de velocidad Tx inferiro a los 12 Mbps a cantides mayores el jitter no aumenta demasiado, pero encontramos una enorme cantidad de tramas perdidas en la red.

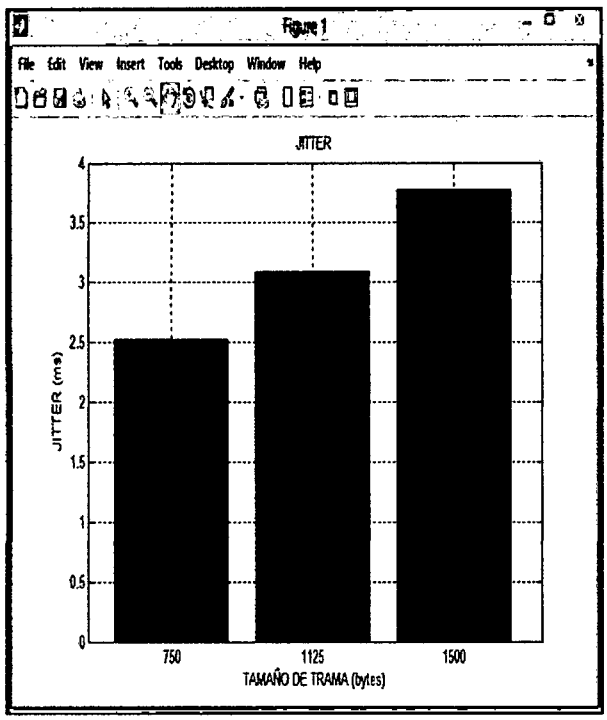


Fig. 4.3.21 Jitter vs. Tamaño de Trama

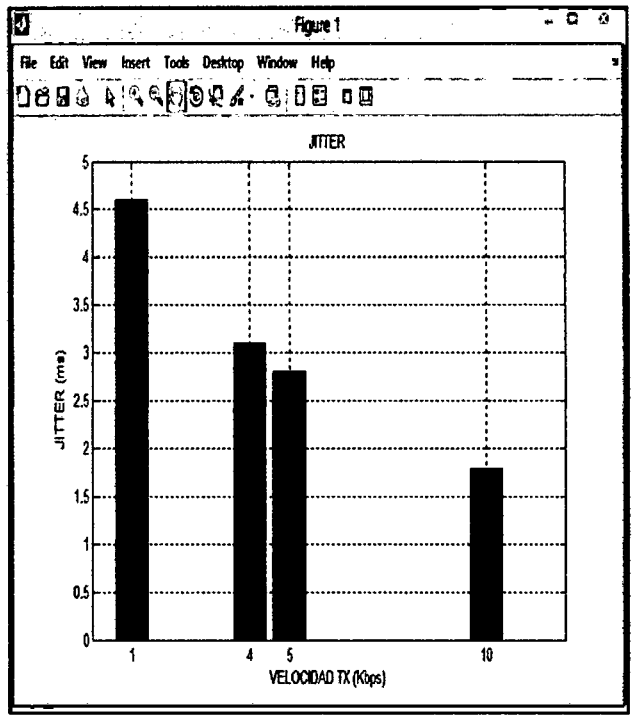


Fig. 4.3.22 Jitter vs. Velocidad Tx

En la figura 4.3.22 se observa los valores del Jitter obtenidos al enviar diferentes tamaños de paquete UDP como 750, 1125 y 1500 bytes utilizando una velocidad de Tx constante de 5 Mbps, se puede observar claramente que con una trama de 750 bytes se tiene un Jitter de 2.52 ms a diferencia de la trama de 1500 bytes en la cual se tiene un Jitter de 3.77 ms.

En la figura 4.2.23, se observa los valores del Jitter obtenidos al enviar paquetes UDP de 1470 bytes utilizando una velocidad de Tx que varía entre 1 Mbps y los 10 Mbps, sin que se pierdan paquetes en la red, se puede observar claramente que con una velocidad Tx de 1 Mbps se tiene un Jitter de 4. 61 ms a diferencia que a una velocidad Tx de 10 Mbps en la cual se tiene un Jitter de 1.78 ms.

Medición de Jitter a 10 Mbps:

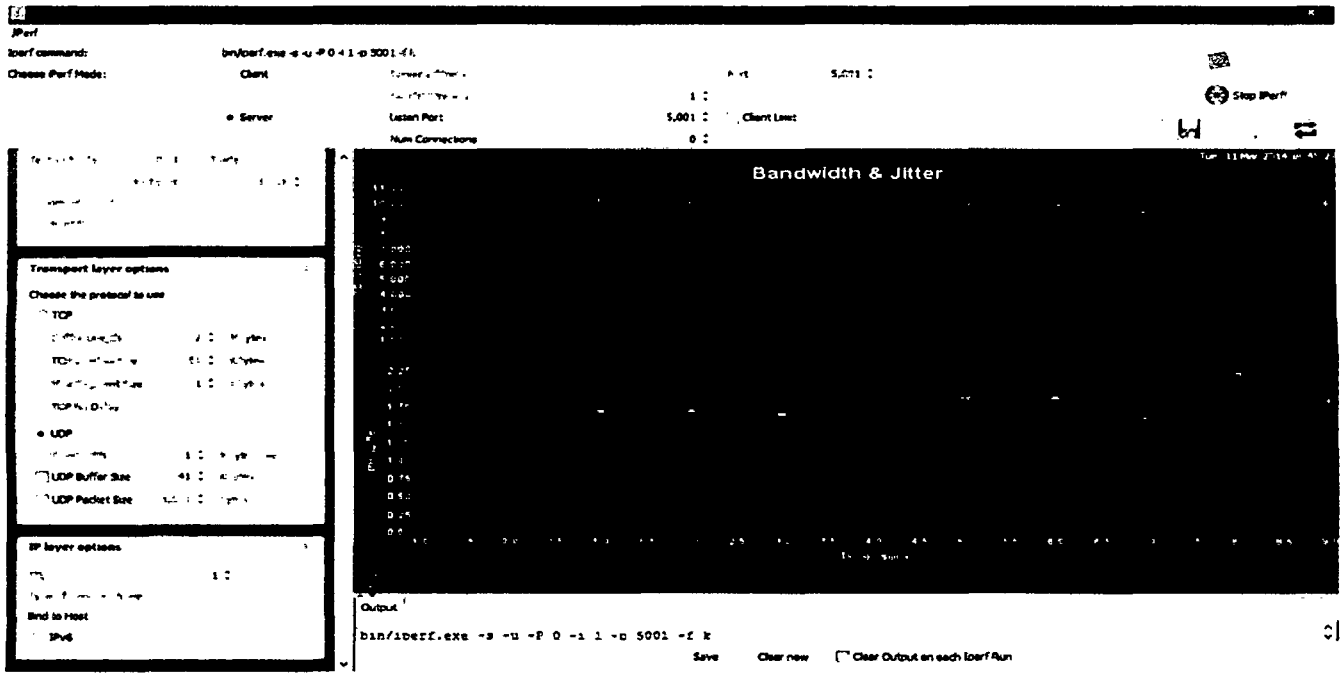


Fig. 4.3.23 Gráfica de Bandwidth y Jitter

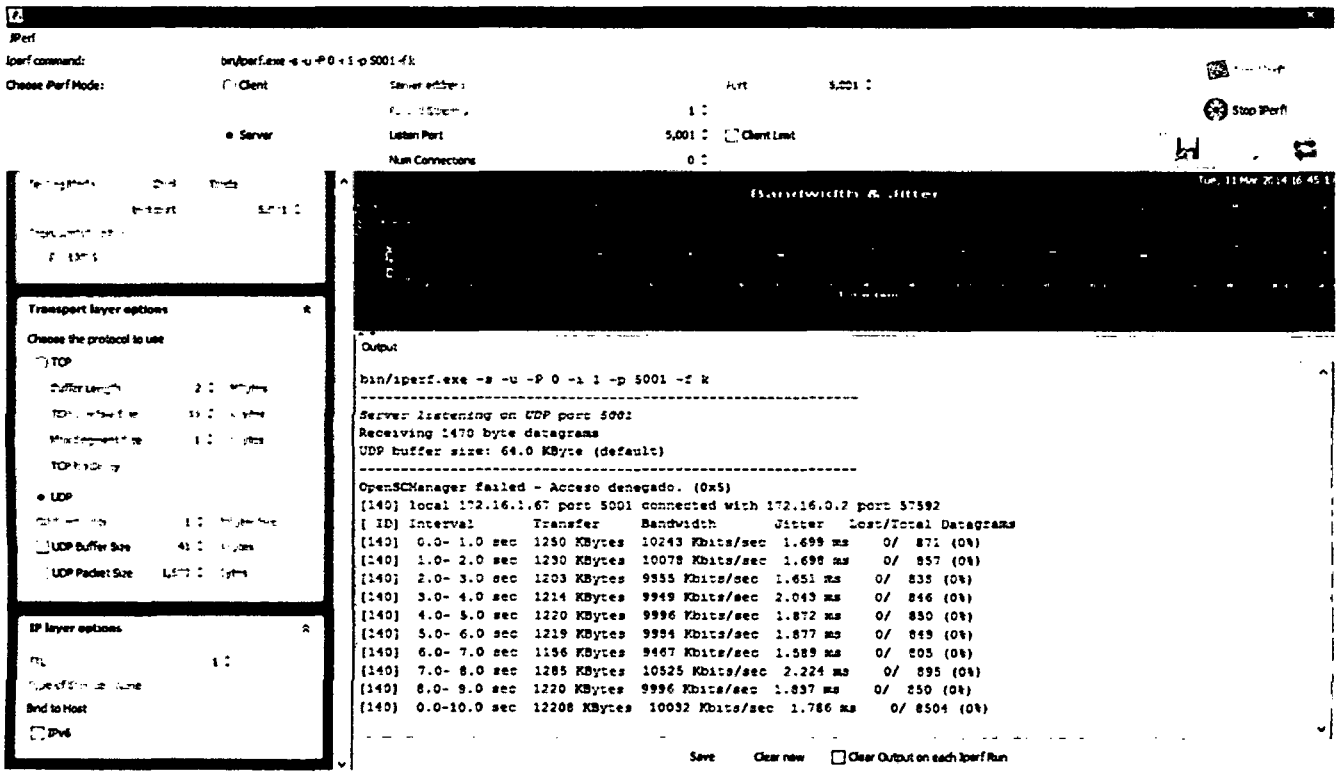


Fig. 4.3.24 Resultados al medir Throughput como servidor

PASO 4: Captura de tráfico con Wireshark.

Capturar tráfico de paquetes en la interfaz f2/0 de R1.

- Captura de paquetes ICMP.

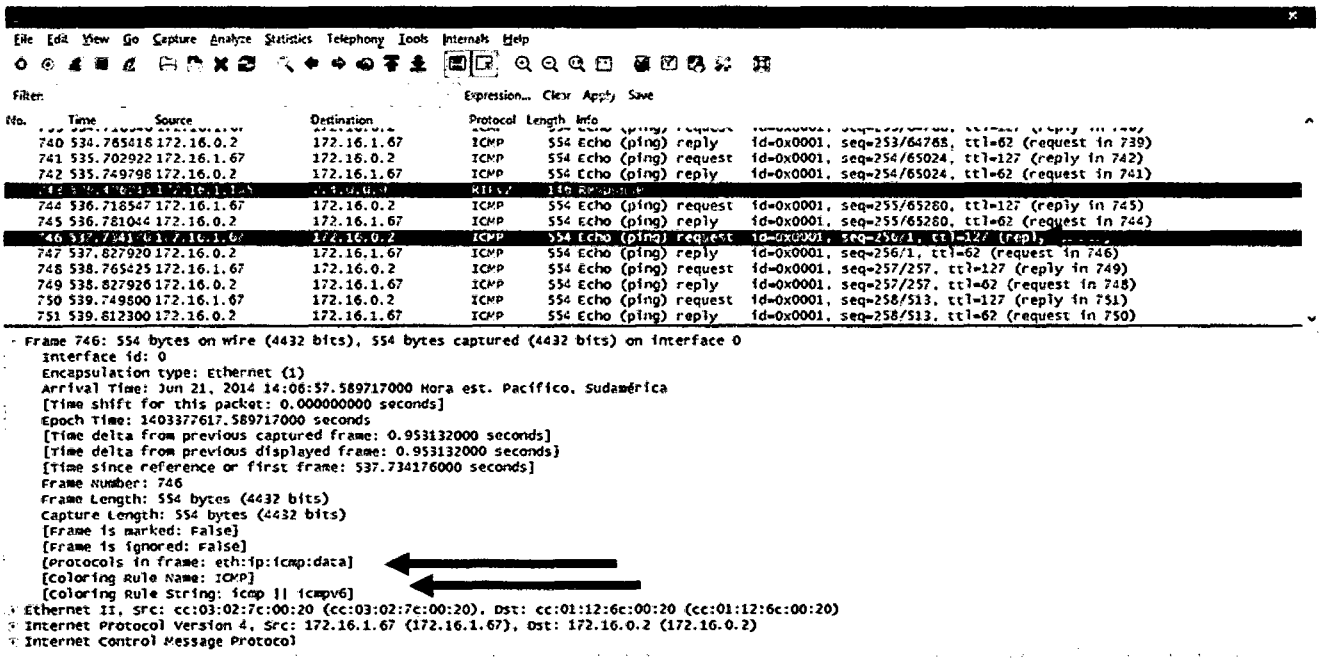


Fig. 4.3.25 Captura de paquetes ICMP con Wireshark

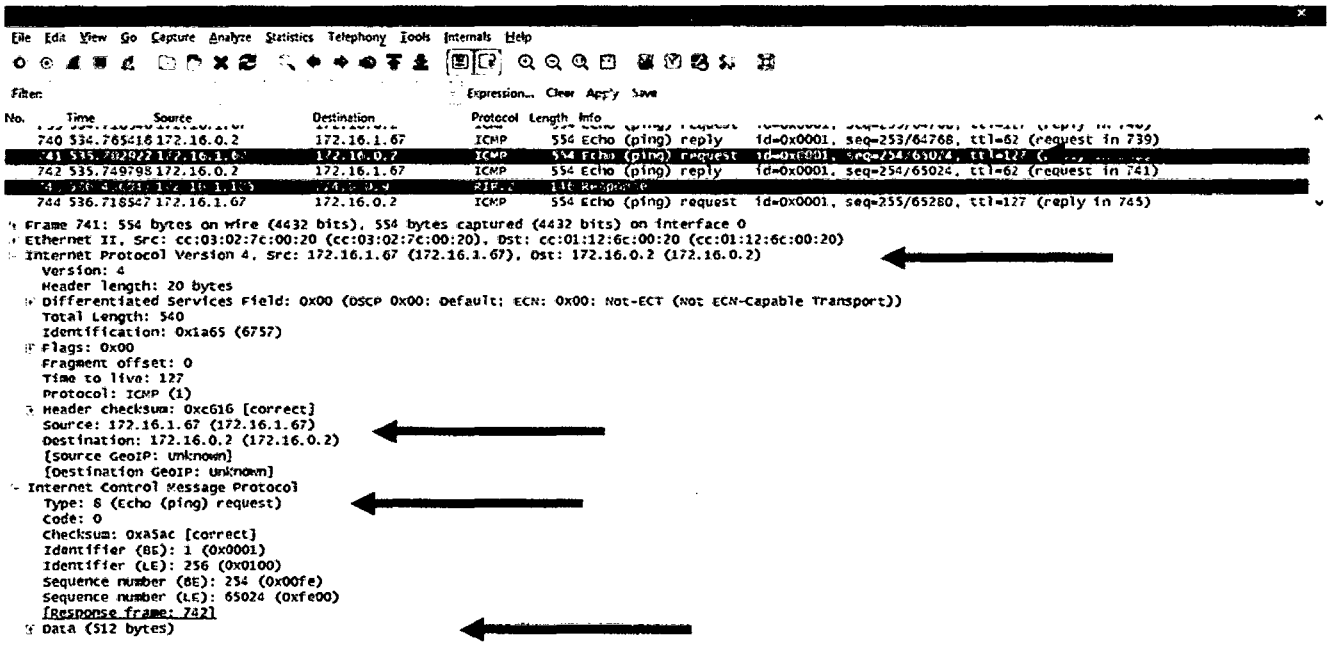


Fig. 4.3.26 Información detallada del paquete ICMP

- Protocolo de enrutamiento RIPv2:

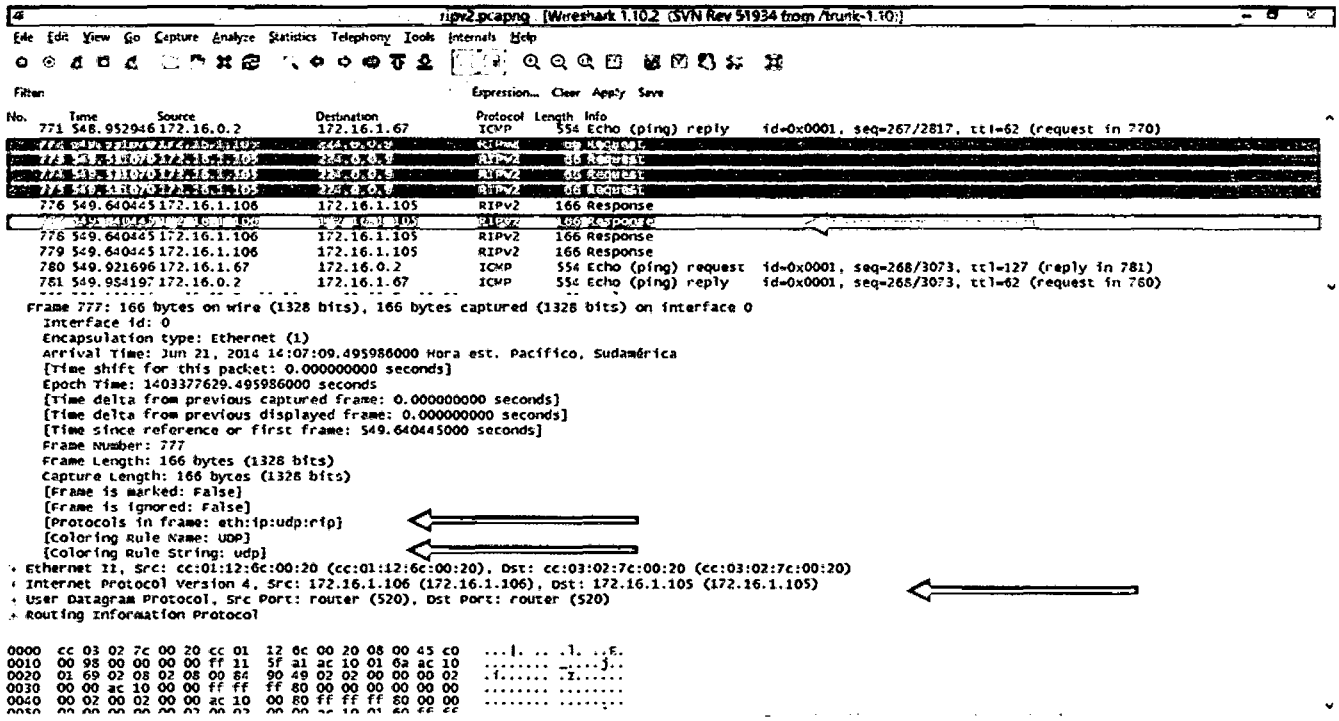


Fig. 4.3.27 Captura del protocolo RIPv2 con Wireshark

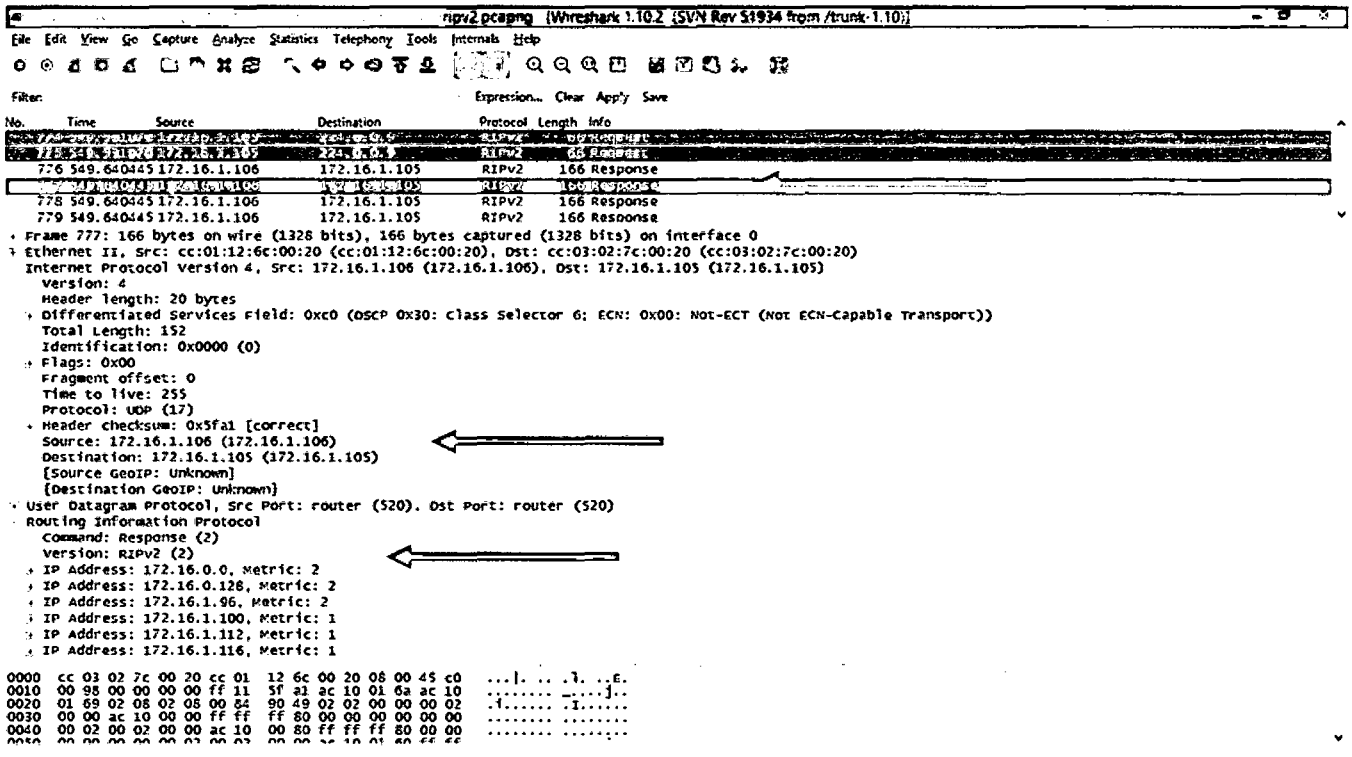


Fig. 4.3.28 Información detallada del protocolo RIPv2.

LABORATORIO 4.4: CONFIGURACION EIGRP

REVISIÓN TEÓRICA: Para la realización de esta práctica se deberá revisar conceptos de enrutamiento EIGRP.

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet.
- Configurar el enrutamiento EIGRP.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **172.16.1.0/16** para obtener el direccionamiento IP usando VLSM para las interfaces seriales y utilizar la dirección **192.168.1.0/24** para **LAN R1**, la dirección **192.168.2.0/24** para **LAN R2** y dirección **192.168.3.0/24** para **LAN R5**, teniendo los siguientes requisitos:

LAN R1: 20 host.
LAN R2: 30 host.
LAN R5: 10 host.

DIAGRAMA DE TOPOLOGIA

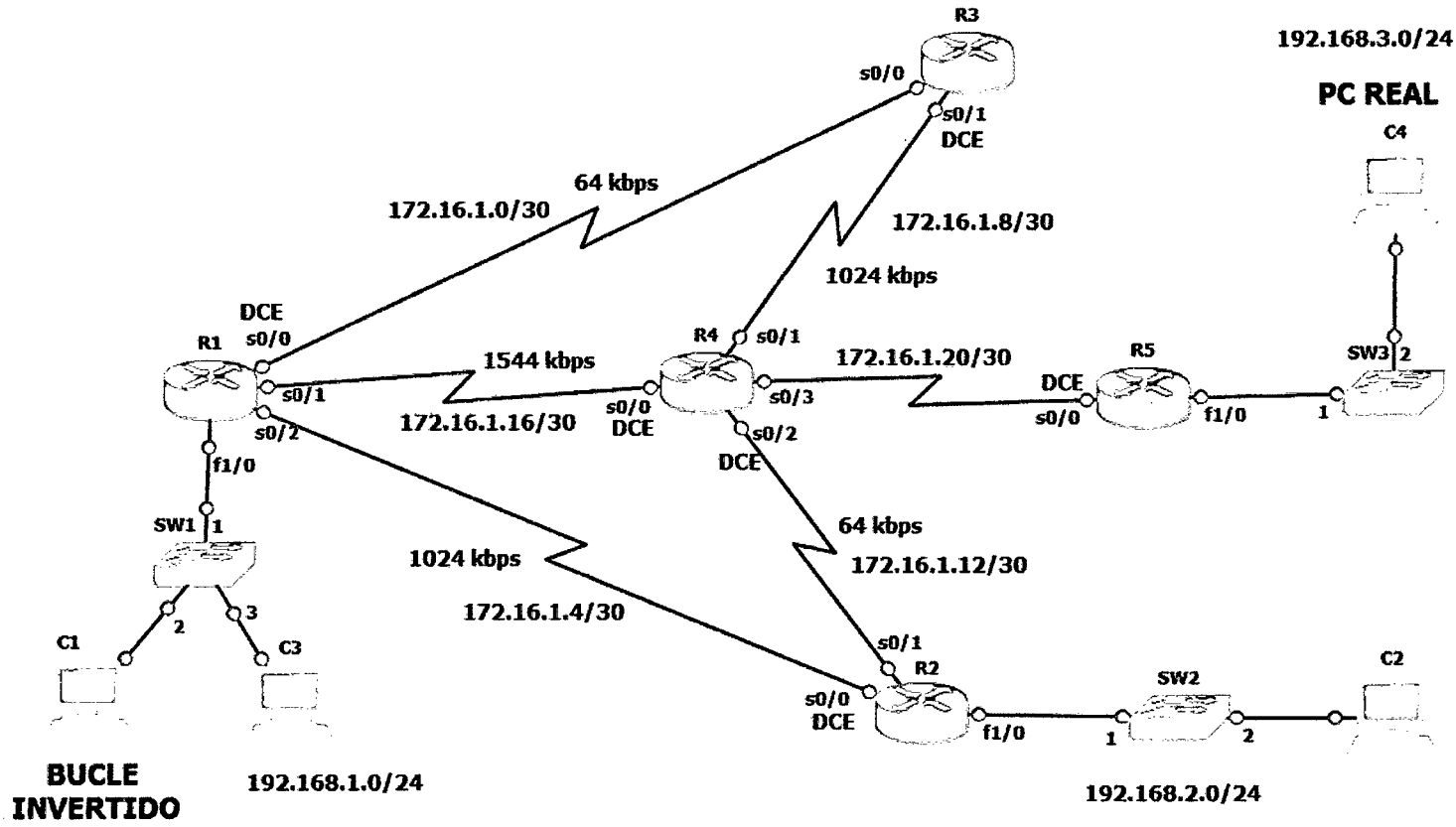


Fig. 4.4.1 Red Virtual en GNS3

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s0/0	172.16.1.1	255.255.255.252	No aplicable
	s0/1	172.16.1.17	255.255.255.252	No aplicable
	s0/2	172.16.1.5	255.255.255.252	No aplicable
	f1/0	192.168.1.1	255.255.255.0	No aplicable
R2	s0/0	172.16.1.6	255.255.255.252	No aplicable
	s0/1	172.16.1.13	255.255.255.252	No aplicable
	f1/0	192.168.2.1	255.255.255.0	No aplicable
R3	s0/0	172.16.1.2	255.255.255.252	No aplicable
	s0/1	172.16.1.9	255.255.255.252	No aplicable
R4	s0/0	172.16.1.18	255.255.255.252	No aplicable
	s0/1	172.16.1.10	255.255.255.252	No aplicable
	s0/2	172.16.1.14	255.255.255.252	No aplicable
	f1/0	172.16.1.21	255.255.255.252	No aplicable
R5	s0/0	172.16.1.22	255.255.255.252	No aplicable
	f1/0	192.168.3.1	255.255.255.0	No aplicable
C1	BUCLE INVERTIDO	192.168.1.2	255.255.255.0	192.168.1.1
C2	VPCS	192.168.2.2	255.255.255.0	192.168.2.1
C3	VPCS	192.168.1.3	255.255.255.0	192.168.1.1
C4	NIC	192.168.3.2	255.255.255.0	192.168.3.1

Tabla 4.4.1 Direccionamiento IP para las Redes

TAREA 1: MONTAR LA RED EN GNS3

Montar y conectar la red igual a la del Diagrama de topología.

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

Ingrese al modo privilegiado

Router>enable

Aparece el siguiente prompt

Router#

En el modo exec privilegiado, ingrese al modo de configuración global:

Router# **configure terminal**

PASO 1: Establezca la configuración global del nombre de host.

Ingrese el siguiente comando para configurar el nombre del router:

Router(config)#**hostname XXXXXX** (Escribir nombre deseado)

PASO 2: Desactive la búsqueda DNS.

Router(config)# **no ip-domain lookup**

Si escribes algo que no sea un comando de Cisco IOS o cometes un error, el router asume que ha escrito un nombre de dominio y trata de resolver lo que usted escribe, realizando una búsqueda de DNS.

PASO 3: Configure un mensaje para que se muestre al ingresar al router.

Router(config)#**banner motd %** Solo acceso a personal autorizado **%** (Puede escribir cualquier mensaje)

El símbolo % indica el inicio y final del mensaje.

PASO 4: Configure las contraseñas de consola, enable secret y VTY.

Seguir los siguientes pasos:

Router(config)# **line console 0**

Router(config-line)# **password XXXXX** (Escribir contraseña deseada)

Router(config-line)# **login**

Router(config-line)# **exit**

Router(config)# **enable secret XXXXX** (Escribir contraseña deseada)

Router(config)# **line vty 0 4**

Router(config-line)# **password XXXXX** (Escribir contraseña deseada)

Router(config-line)# **login**

Router(config-line)# **exit**

PASO 5: Sincronice los mensajes no solicitados y el resultado de la depuración con el resultado solicitado y los indicadores para las líneas de consola y de terminal virtual.

Router(config)# **line console 0**

Router(config)# **logging synchronous**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **logging synchronous**

Router(config)# **exit**

PASO 6: Configure un tiempo de espera EXEC de 10 minutos.

Router(config)# **line console 0**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

PASO 7: Guardar la configuración.

Router(config)# **copy running-config startup-config**

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET.

Aplique Los siguientes comandos:

R1:

Configuración para una interface serial:

R1(config)# **interface serial 0/0**

R1(config-if)# **description conexion a R3**

R1(config-if)# **ip address 172.16.1.1 255.255.255.252**

R1(config-if)# **clock rate 64000**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface serial 0/1**

R1(config-if)# **description conexion a R4**

R1(config-if)# **ip address 172.16.1.17 255.255.255.252**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface serial 0/2**

R1(config-if)# **description conexion a R2**

R1(config-if)# **ip address 172.16.1.5 255.255.255.252**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

Configuración para una interface fasEthernet:

R1(config)# **interface fasEthernet 1/0**

R1(config-if)# **description conexion a LAN 1**

R1(config-if)# **ip address 192.168.1.1 255.255.255.0**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

NOTA: Seguir los mismos pasos para los demás routers con sus respectivos parámetros.

TAREA 4: CONFIGURAR EIGRP.

PASO 1: Para configurar EIGRP, Utilice el comando.

Router(config)#router eigrp [autonomous-system]

Router(config-router)#network [network-adress] [wildcard-mask]

R1:

R1(config)# **router eigrp 1**

R1(config-router)# **network 172.16.1.0 0.0.0.3**

R1(config-router)# **network 172.16.1.4 0.0.0.3**

R1(config-router)# **network 172.16.1.16 0.0.0.3**

R1(config-router)# **network 192.168.1.0 0.0.0.255**

R1(config-router)# **exit**

NOTA: Seguir los mismos pasos para los demás routers con sus correspondientes redes.

PASO 2: Modificar bandwidth.

R1:

R1(config)# **interface serial 0/0**

R1(config-if)# **bandwidth 64**

R1(config-if)# **exit**

R1(config)# **interface serial 0/1**

R1(config)# **bandwidth 1544**

R1(config-if)# **exit**

R1(config)# **interface serial 0/2**

R1(config)# **bandwidth 1024**

R1(config)# **end**

TAREA 5: CONFIGURAR LOS EQUIPOS DE HOST.

VPCS

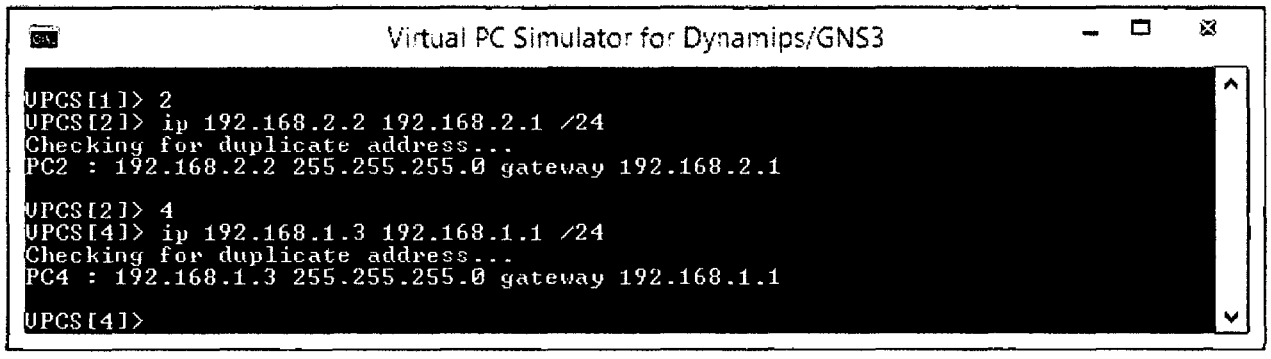


Fig. 4.4.2 Configuración de IP para VPCS.

PC REAL

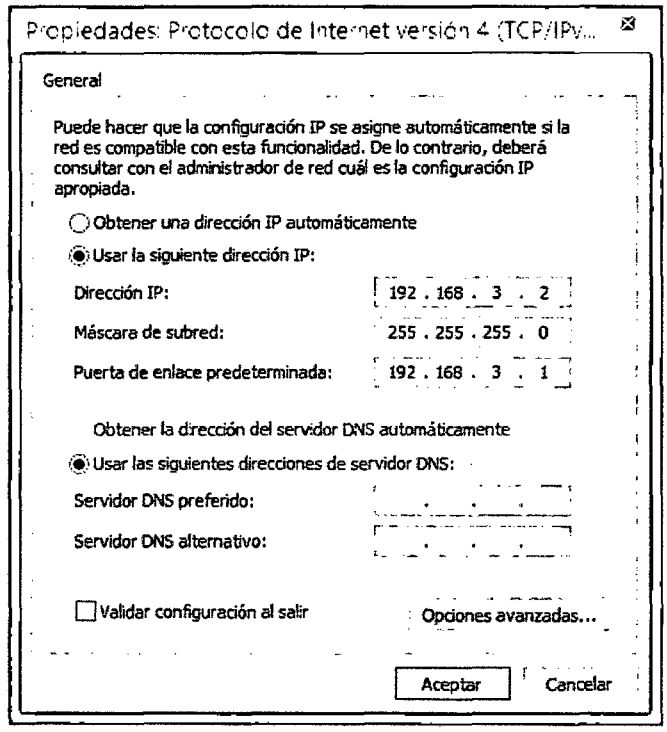


Fig. 4.4.3 Configuración de IP para PC REAL.

NOTA: Configurar los demás host.

TAREA 6: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

PASO 1: Verificar configuraciones.

R4#**show ip route**

Muestra el contenido de la tabla de enrutamiento IP.

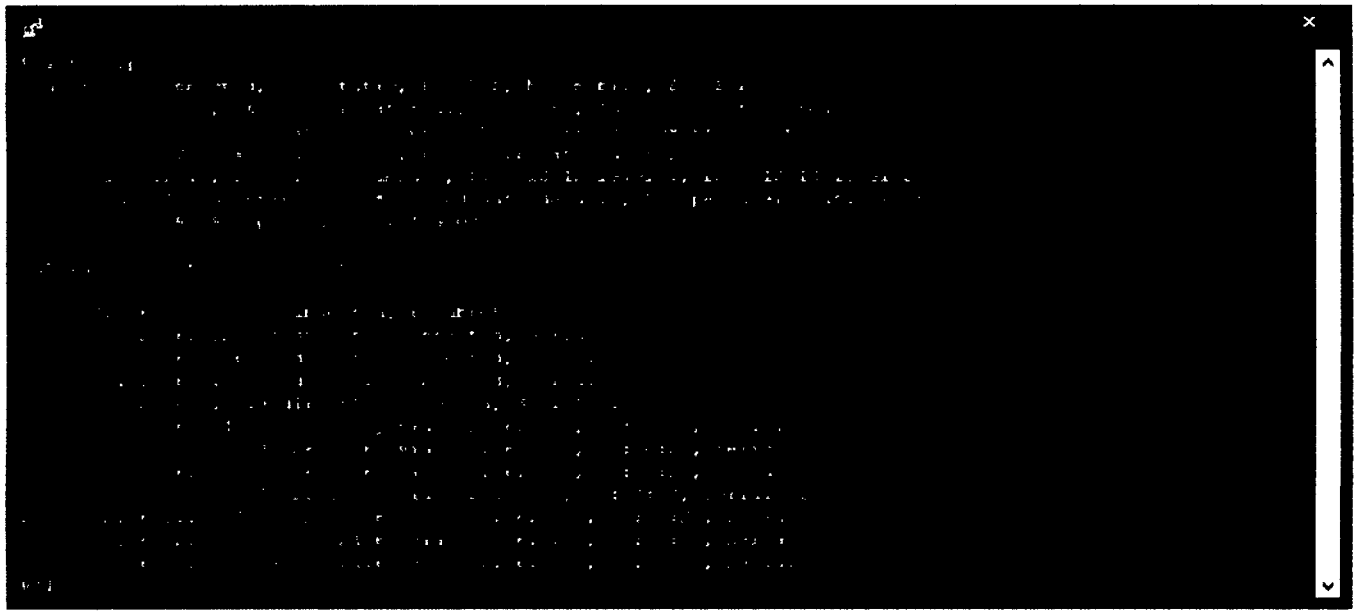


Fig. 4.4.4 Tabla de enrutamiento de R4.

R4# **show ip protocols**

Muestra los parámetros del protocolo, como AS, valores de los parámetros K1, K3, el valor de AD, etc.

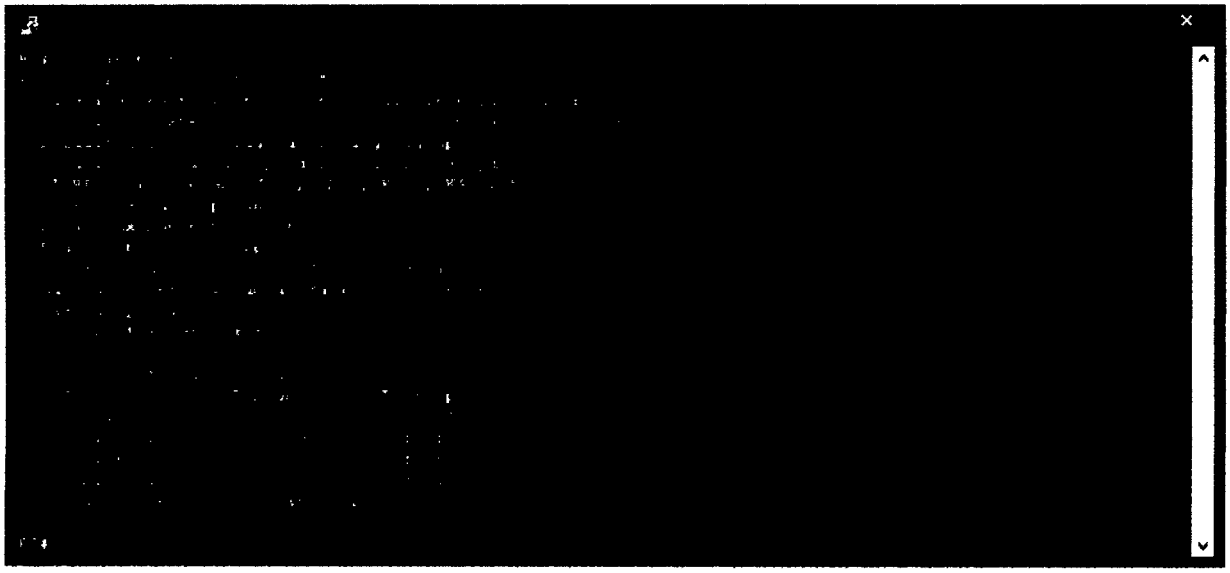


Fig. 4.4.5 Tabla de Protocolos.

R4# show ip eigrp neighbors

Muestra las adyacencias o vecindades de un router.

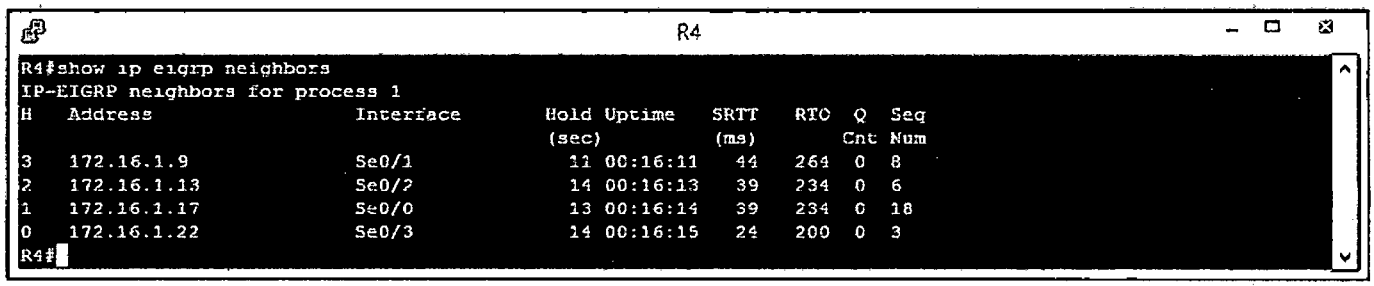


Fig. 4.4.6 Tabla ip eigrp neighbors.

R4# show ip eigrp traffic

Permite visualizar cuantos paquetes de mensajes EIGRP se están enviando: consulta, respuesta, acuse de recibo, saludos.

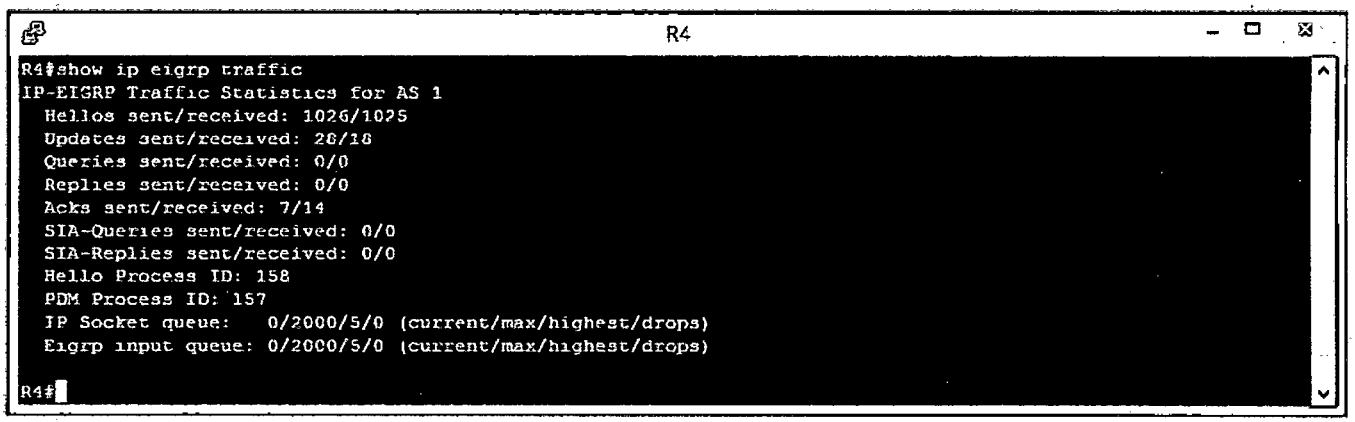


Fig. 4.4.7 Tabla ip eigrp traffic.

R4# show ip interface brief

Muestra un breve resumen de la información y del estado de una dirección IP.

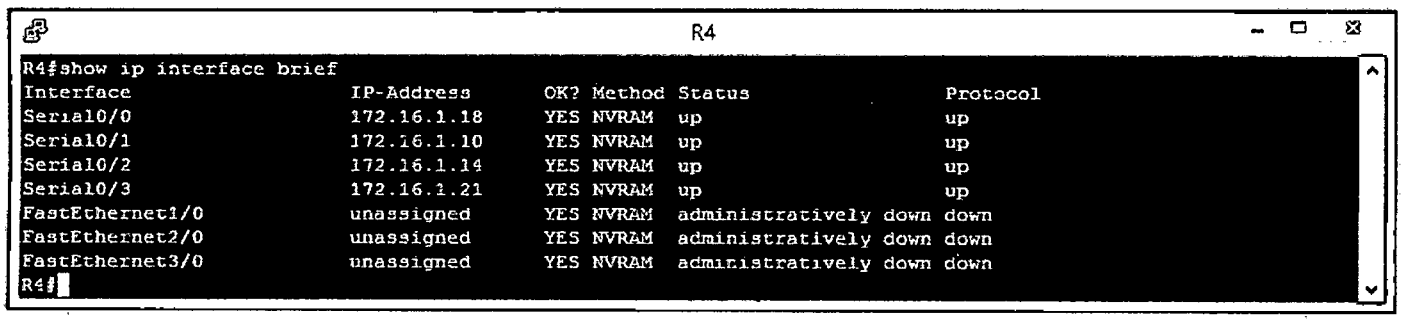


Fig. 4.4.8 Tabla ip interface brief.

R4# **show ip eigrp topology**

Muestra la tabla topológica, en donde encontramos su FD.

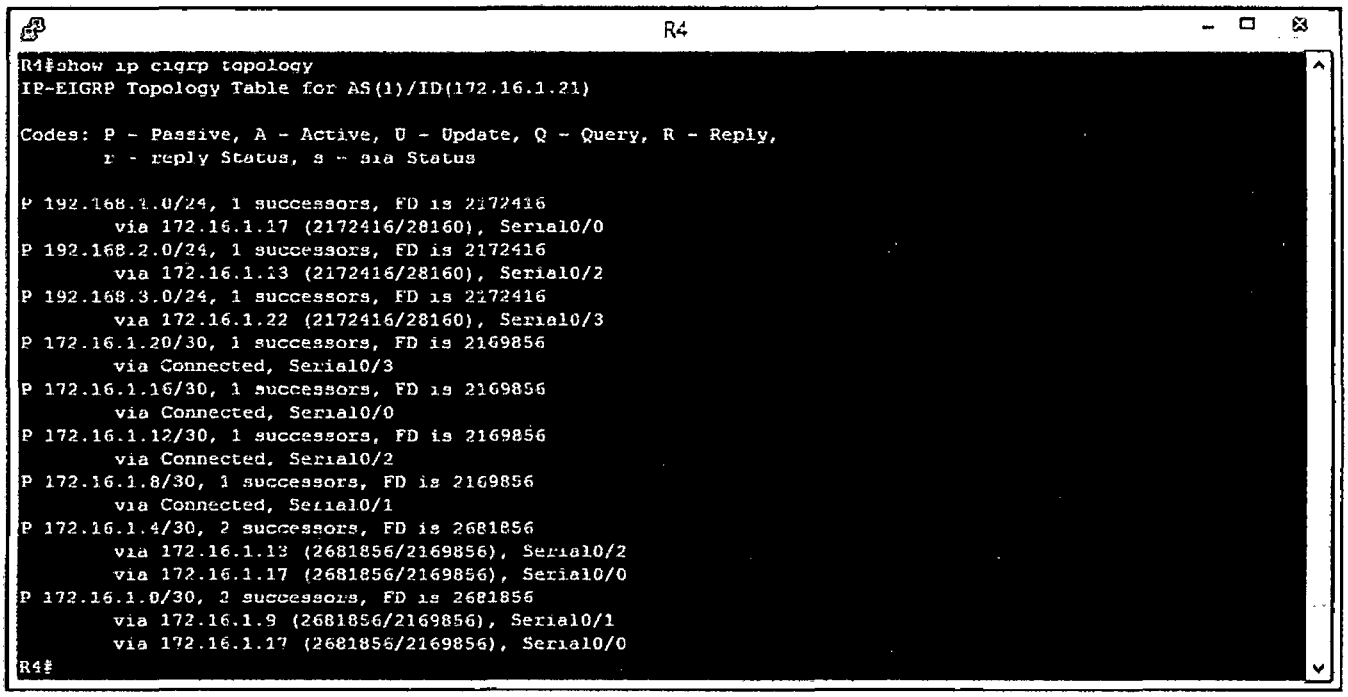


Fig. 4.4.9 Tabla ip eigrp topology.

R4# **show running-config**

Muestra la configuración actual en la RAM.

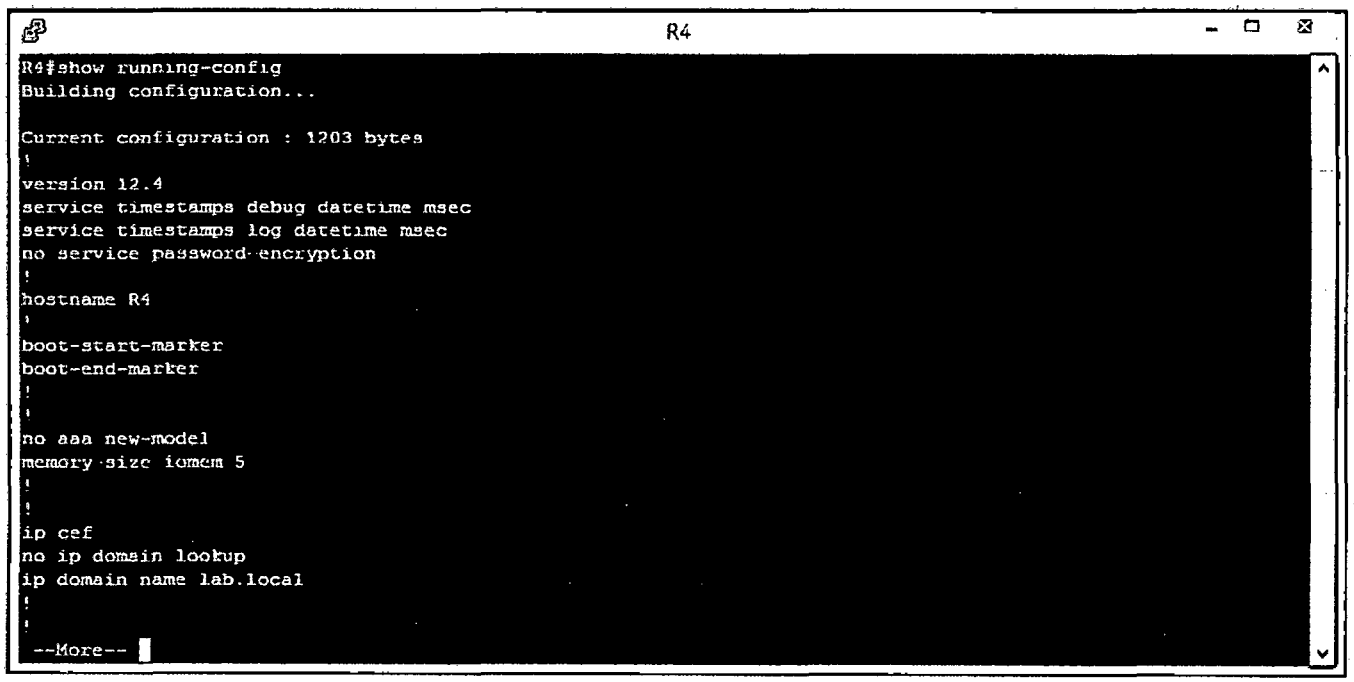


Fig. 4.4.10 Tabla show running-config.

PASO 2: Utilice el comando ping para probar la conectividad entre los routers que no están directamente conectados y también la conectividad entre host.

PING ENTRE ROUTERS

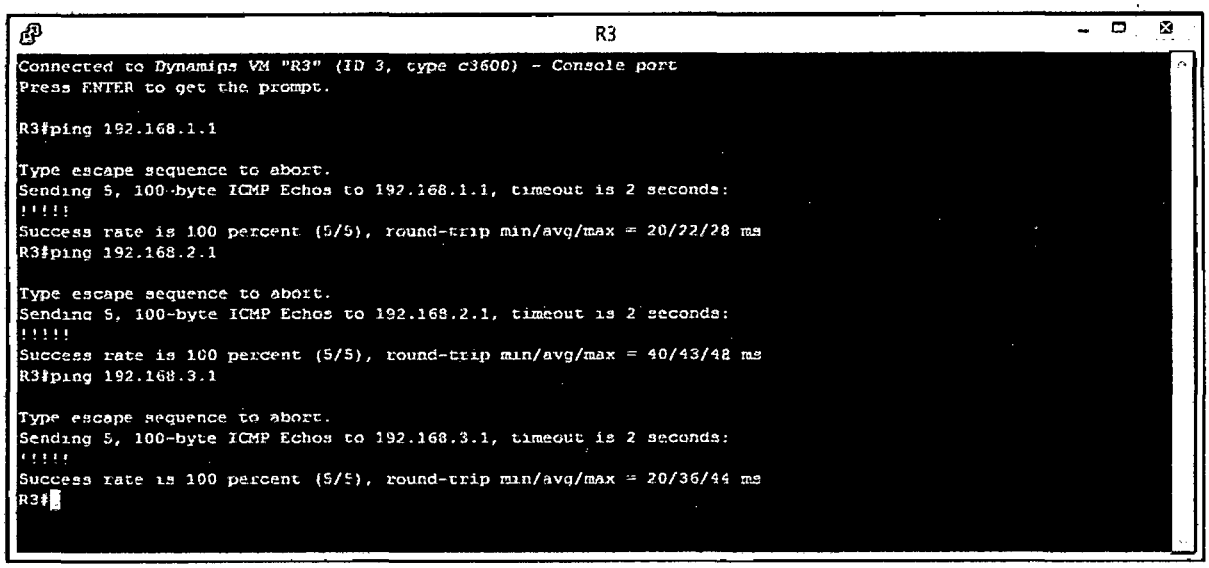


Fig. 4.4.11 Prueba de conectividad entre routers.

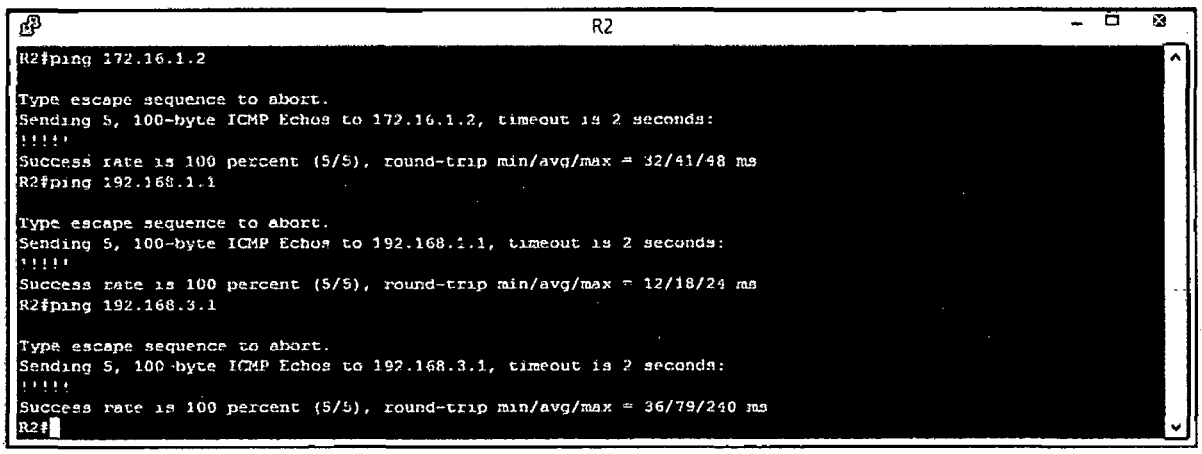
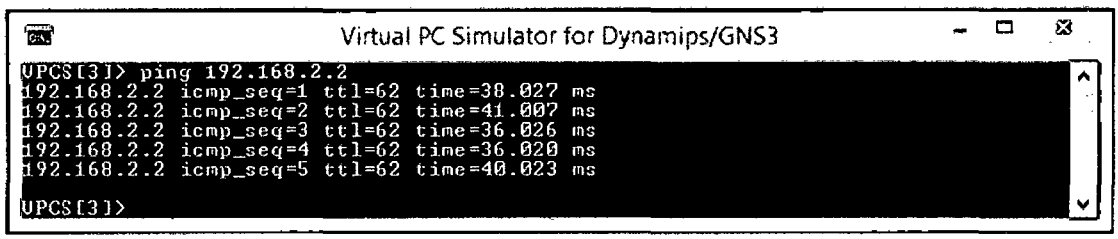


Fig. 4.4.12 Prueba de conectividad entre routers.



PING ENTRE HOST

Fig. 4.4.13 Prueba de conectividad entre host.

NOTA: Realizar las pruebas faltantes.

TAREA 7: ANALIS DEL TRAFICO DE PAQUETES

PASO 1: Medición de la Latencia

Para la medición de la latencia se realizó 10 muestras sucesivas de 100 ping desde el C1 (Bucle invertido) hacia la PC REAL considerando un tamaño de trama de 64, 512 y 1518 bytes como se especifica en el RFC 2544.

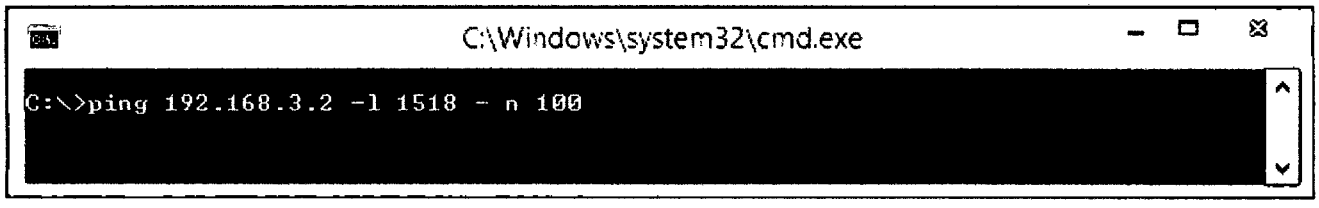


Fig. 4.4.14 Forma de medición de la latencia.

En la Figura 4.4.14 se puede observar el envío de 100 ping con una trama de 1518 hacia la dirección 192.168.3.2

En las Tablas posteriores se detallan los valores de la Latencia que se ha obtenido una vez realizadas todas las muestras.

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	**80**	**110**	**115**	**111**	**114**	**115**	**117**	**110**	**115**	**111**	**109.8**
Tiempo Máximo (ms)	**188**	**141**	**124**	**127**	**135**	**126**	**124**	**130**	**123**	**130**	**134.8**
Tiempo Promedio (ms)	**124**	**122**	**117**	**121**	**120**	**122**	**120**	**121**	**119**	**123**	**120.9**

Tabla 4.4.2 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	512										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	111	116	114	112	116	117	111	113	112	111	113.3
Tiempo Máximo (ms)	129	198	193	129	151	123	129	135	129	130	144.6
Tiempo Promedio (ms)	119	122	121	119	121	120	120	119	121	123	120.5

Tabla 4.4.3 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1518										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	147	142	146	142	145	145	142	145	142	144	144
Tiempo Máximo (ms)	167	160	165	159	154	164	158	161	159	270	171.7
Tiempo Promedio (ms)	152	151	149	152	148	151	154	149	154	155	151.5

Tabla 4.4.4 Datos obtenidos para una trama de 1518 bytes.

LATENCIA			
Tamaño de Trama (bytes)	64	512	1518
Tiempo Mínimo (ms)	109.8	113.3	144
Tiempo Máximo (ms)	134.8	144.6	171.7
Tiempo Promedio (ms)	120.9	120.5	151.5

Tabla 4.4.5 Comparación de datos obtenidos de las diferentes tramas.

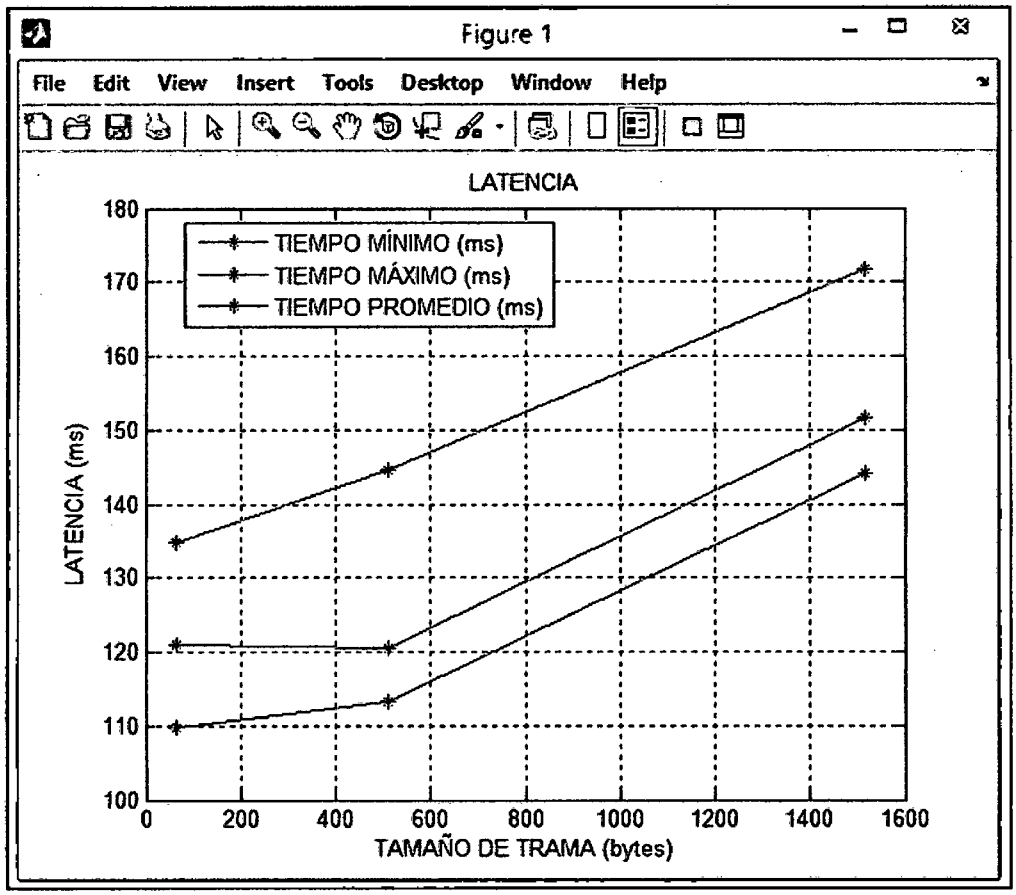


Fig. 4.4.15 Datos representados gráficamente de la variación de la latencia.

De acuerdo con los datos obtenidos, se puede observar claramente que los valores mínimo (color azul), máximo (color rojo) y promedio (color verde) de la latencia de la red se incrementan conforme se envía una trama de longitud mayor, en este caso con la trama de 1518 bytes se obtiene una latencia promedio de 151.5 ms a diferencia de una trama de 64 bytes con 120.9 ms.

PASO 2: Medición del Throughput

Para la medición del Throughput y Jitter se envió una cantidad de tramas a velocidades diferentes durante 20 segundos, hasta encontrar la máxima cantidad de tramas recibidas sin que se produzcan perdidas de las mismas en el router y PC REAL. Como se utilizó Jperf el cliente será el encargado de enviar los paquetes y el servidor los recibirá, indicando la cantidad de paquetes que llegaron correctamente considerando un tamaño del paquete UDP de 750, 1125, 1500 y 1470 (default) bytes, tal como se especifica en el RFC 768.

Configuración del Jperf como servidor con UDP Packet Size de 750 Bytes.

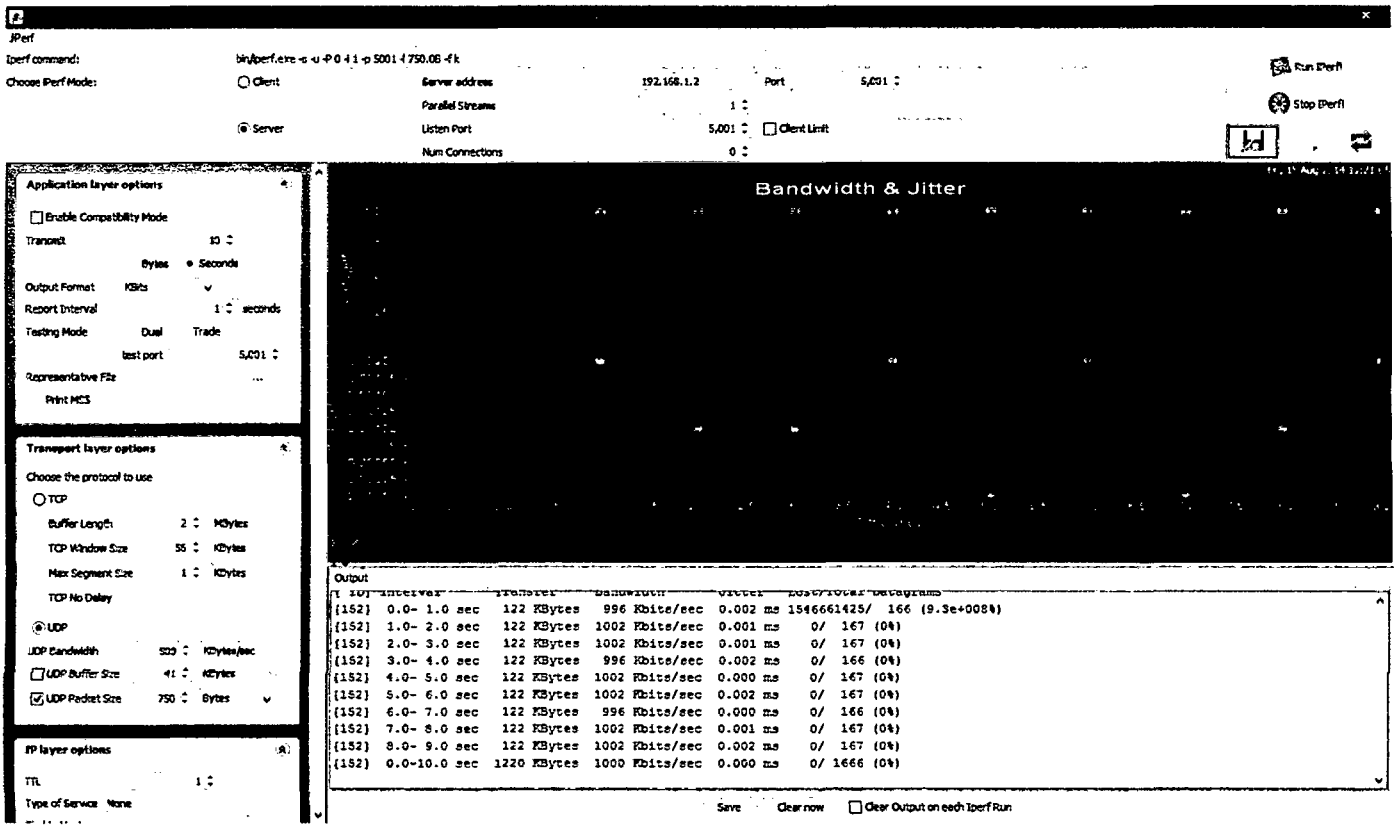


Fig. 4.4.16 Gráfica de Bandwidth y Jitter.

```
bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -l 750.0B -f k
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 750 byte datagrams
UDP buffer size: 64.0 KByte (default)
------------------------------------------------------------
OpenSCManager failed - Acceso denegado. (0x5)
[152] local 192.168.3.2 port 5001 connected with 169.254.35.253 port 50976
[ ID] Interval       Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[152]  0.0- 1.0 sec   122 KBytes   996 Kbits/sec  0.002 ms 1546661425/  166 (9.3e+008%)
[152]  1.0- 2.0 sec   122 KBytes  1002 Kbits/sec  0.001 ms    0/  167 (0%)
[152]  2.0- 3.0 sec   122 KBytes  1002 Kbits/sec  0.001 ms    0/  167 (0%)
[152]  3.0- 4.0 sec   122 KBytes   996 Kbits/sec  0.002 ms    0/  166 (0%)
[152]  4.0- 5.0 sec   122 KBytes  1002 Kbits/sec  0.000 ms    0/  167 (0%)
[152]  5.0- 6.0 sec   122 KBytes  1002 Kbits/sec  0.002 ms    0/  167 (0%)
[152]  6.0- 7.0 sec   122 KBytes   996 Kbits/sec  0.000 ms    0/  166 (0%)
[152]  7.0- 8.0 sec   122 KBytes  1002 Kbits/sec  0.001 ms    0/  167 (0%)
[152]  8.0- 9.0 sec   122 KBytes  1002 Kbits/sec  0.002 ms    0/  167 (0%)
[152]  0.0-10.0 sec  1220 KBytes  1000 Kbits/sec  0.000 ms    0/ 1666 (0%)
```

Fig. 4.4.17 Resultados al medir como servidor.

Configuración del Jperf como cliente con UDP Bandwidth de 1 Mbps y UDP Packet Size de 750 Bytes.

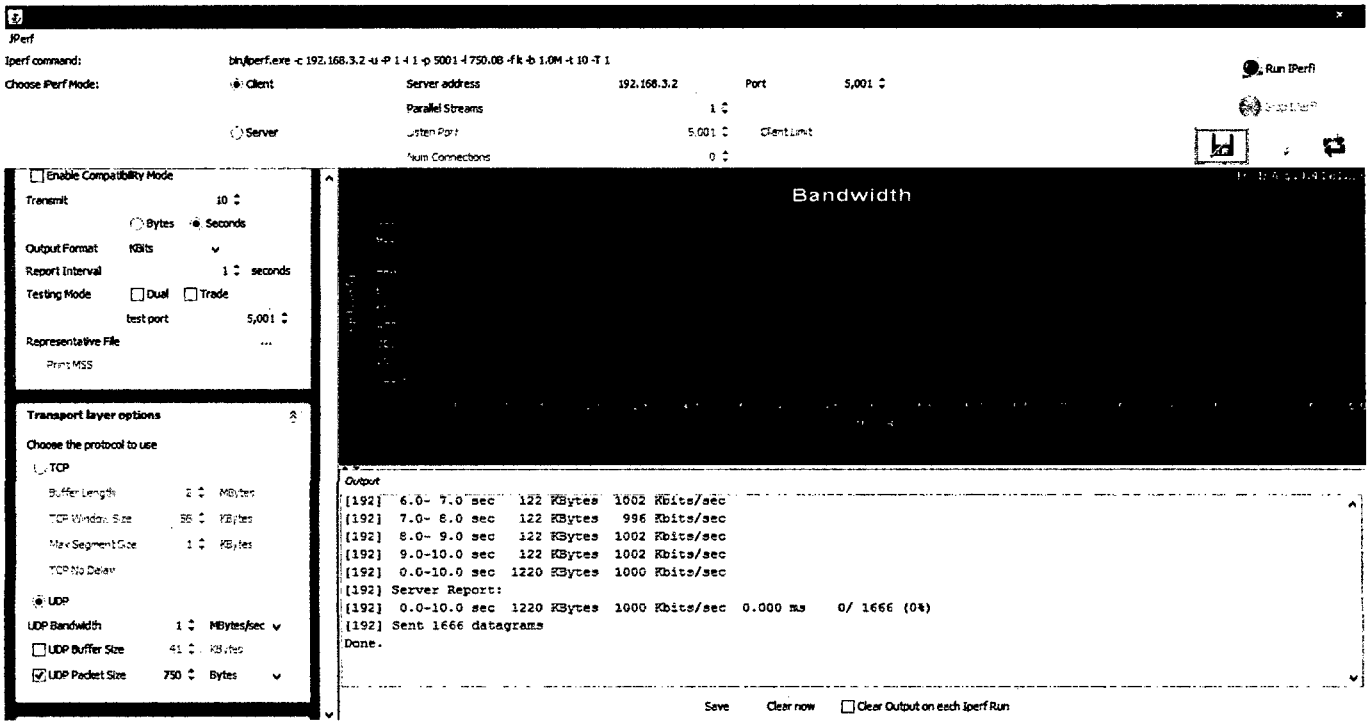


Fig. 4.4.18 Resultados del Jperf como Cliente.

En las siguientes Tablas se detalla los valores del Throughput obtenidos una vez realizada todas las muestras.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**1**	**1**	**1**
Velocidad de Rx (Mbps)	**1**	**1**	**1**
Tramas Transmitidas	**1666**	**1111**	**834**
Tramas Recibidas	**1666**	**1111**	**834**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**166.6**	**111.1**	**83.4**

Tabla 4.4.6 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**0.5**	**0.8**	**1**
Velocidad de Rx (Mbps)	**0.5**	**0.8**	**1**
Tramas Transmitidas	**426**	**681**	**851**
Tramas Recibidas	**426**	**681**	**851**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**42.6**	**68.1**	**85.1**

Tabla 4.4.7 *Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.*

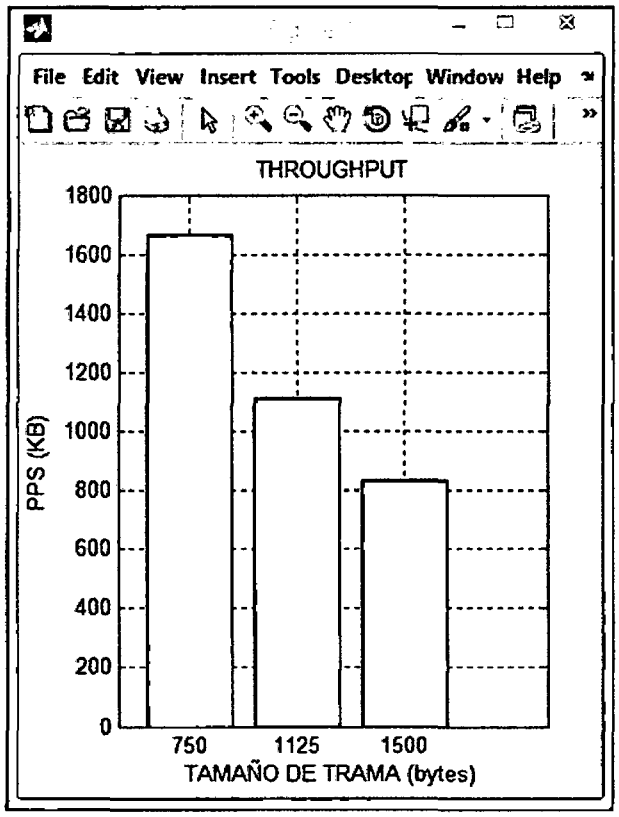


Fig. 4.4.19 PPS vs. Tamaño de Trama.

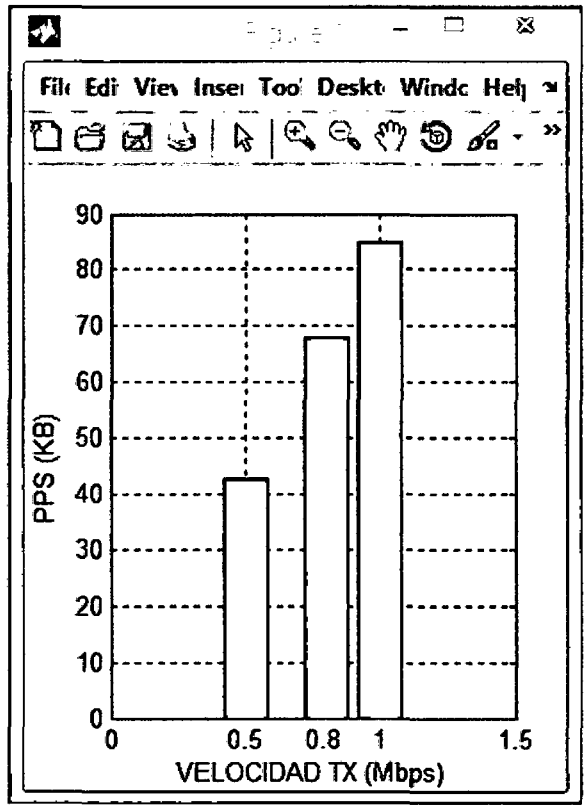


Fig. 4.4.20 PPS vs. Velocidad Tx.

En la figura 4.4.19, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 750 bytes, 1125 bytes y 1500 bytes los cuales han utilizado una velocidad de Tx constante de 1 Mbps, en la gráfica se puede observar claramente que al enviar una trama de 750 bytes se envía 1666 pps, con una trama de 1125 se envía 1111 pps y con una trama de 1500 se envía 834 pps.

Mientras en la figura 4.4.20, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 1470 bytes los cuales han utilizado una velocidad de Tx variada de: 0.5 Mbps, 0.8 Mbps y 1 Mbps, sin que se produzcan perdidas en el envío, como los datos que se muestran en la tabla 4.4.7.

PASO 3: Medición del Jitter

Para la medición se envió datos UDP de longitud variable a velocidades diferentes de Throughput obtenida anteriormente durante 20 segundos. Como se utilizó anteriormente Jperf el cliente será el encargado de enviar los datos y el servidor los recibirá, indicando los valores de Jitter obtenidos durante la transmisión de los datos.

Configuración del Jperf como servidor con UDP Packet Size por defecto.

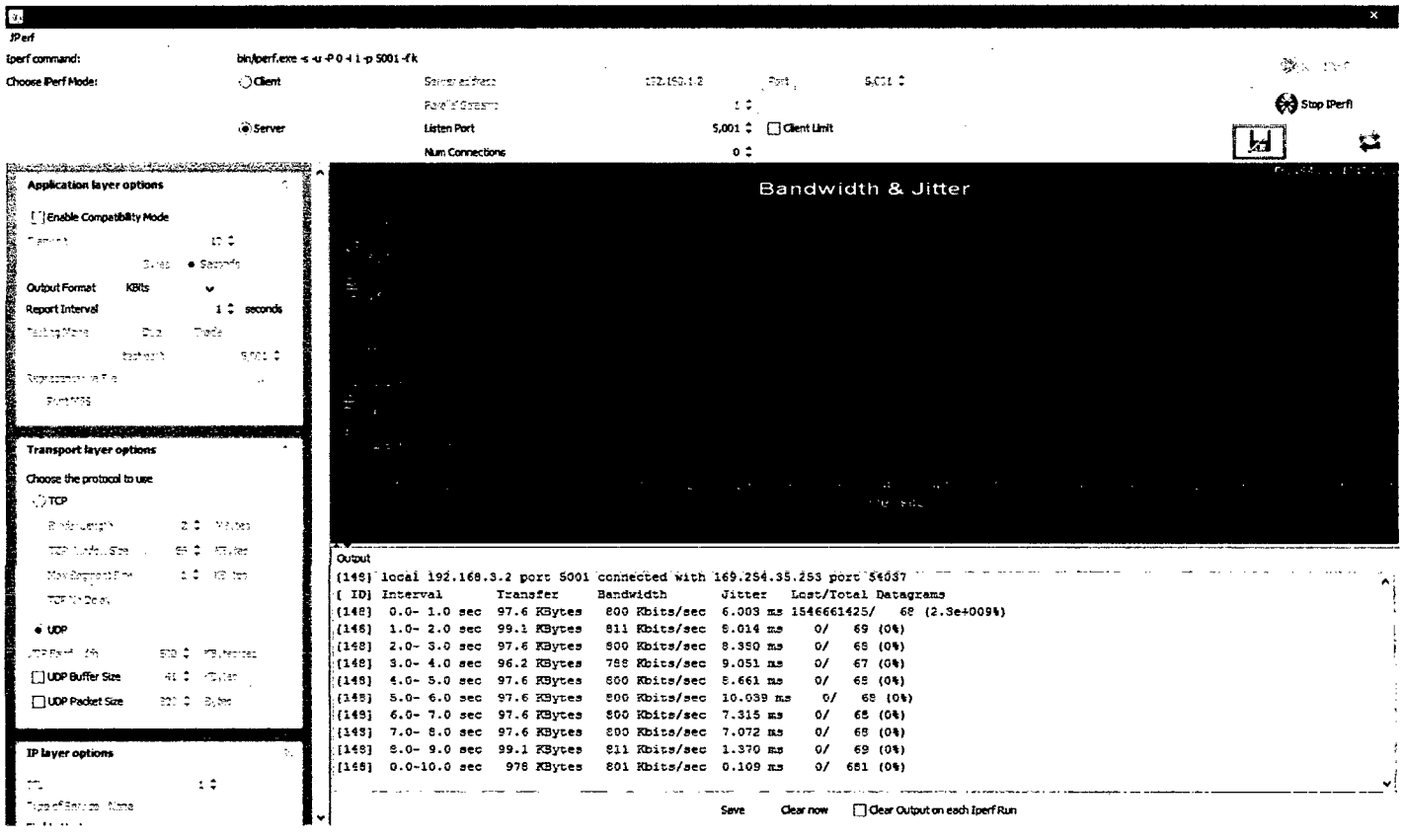


Fig. 4.4.21 Gráfica de Bandwidth y Jitter.

```
bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -f k
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 64.0 KByte (default)
------------------------------------------------------------
OpenSCManager failed - Acceso denegado. (0x5)
[148] local 192.168.3.2 port 5001 connected with 169.254.35.253 port 54037
[ ID] Interval       Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[148]  0.0- 1.0 sec  97.6 KBytes   800 Kbits/sec  6.003 ms 1546661425/   68 (2.3e+009%)
[148]  1.0- 2.0 sec  99.1 KBytes   811 Kbits/sec  8.014 ms    0/   69 (0%)
[148]  2.0- 3.0 sec  97.6 KBytes   800 Kbits/sec  8.380 ms    0/   68 (0%)
[148]  3.0- 4.0 sec  96.2 KBytes   788 Kbits/sec  9.051 ms    0/   67 (0%)
[148]  4.0- 5.0 sec  97.6 KBytes   800 Kbits/sec  8.661 ms    0/   68 (0%)
[148]  5.0- 6.0 sec  97.6 KBytes   800 Kbits/sec  10.039 ms    0/   68 (0%)
[148]  6.0- 7.0 sec  97.6 KBytes   800 Kbits/sec  7.315 ms    0/   68 (0%)
[148]  7.0- 8.0 sec  97.6 KBytes   800 Kbits/sec  7.072 ms    0/   68 (0%)
[148]  8.0- 9.0 sec  99.1 KBytes   811 Kbits/sec  1.370 ms    0/   69 (0%)
[148]  0.0-10.0 sec   978 KBytes   801 Kbits/sec  0.109 ms    0/  681 (0%)
```

Fig. 4.4.22 Resultados al medir como servidor.

En las siguientes Tablas se detalla los valores del Jitter obtenidos una vez realizada todas las muestras.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**1**	**1**	**1**
Velocidad de Rx (Mbps)	**1**	**1**	**1**
Tramas Transmitidas	**1666**	**1111**	**834**
Tramas Recibidas	**1666**	**1111**	**834**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**0.000**	**0.060**	**0.139**

Tabla 4.4.8 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**0.5**	**0.8**	**1**
Velocidad de Rx (Mbps)	**0.5**	**0.8**	**1**
Tramas Transmitidas	**1666**	**1111**	**834**
Tramas Recibidas	**1666**	**1111**	**834**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**0.002**	**0.109**	**1.206**

Tabla 4.4.9 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

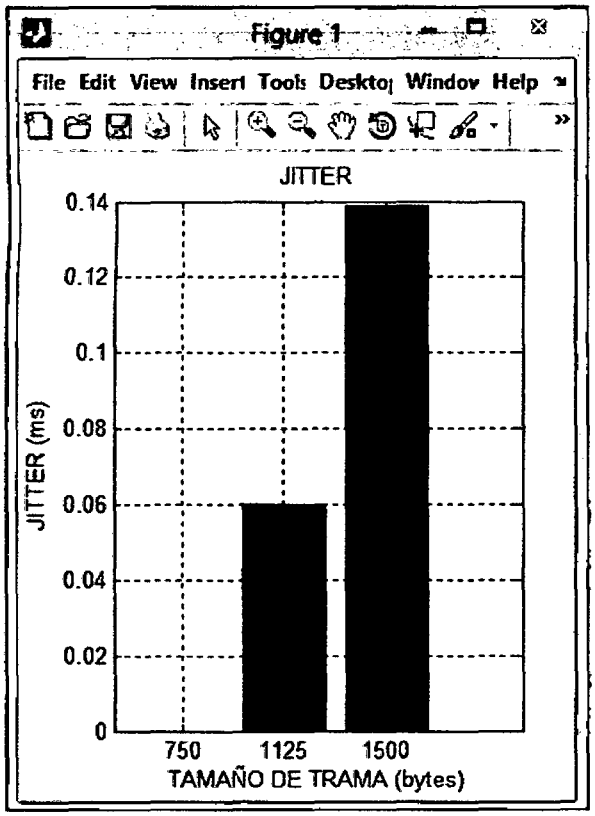


Fig. 4.4.23 Jitter vs. Tamaño de Trama

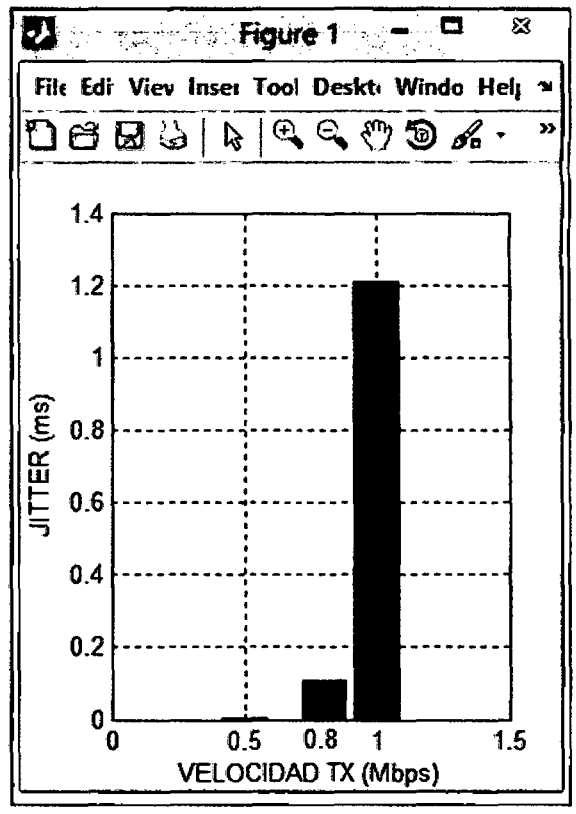


Fig. 4.4.24 Jitter vs. Velocidad Tx

En la figura 4.4.23 se observa los valores del Jitter obtenidos al enviar diferentes tamaños de paquete UDP como 750, 1125 y 1500 bytes utilizando una velocidad de Tx constante de 1 Mbps, se puede observar claramente que con una trama de 750 bytes se tiene un Jitter de 0 ms a diferencia de la trama de 1500 bytes en la cual se tiene un Jitter de 0.139 ms.

En la figura 4.4.24, se observa los valores del Jitter obtenidos al enviar paquetes UDP de 1470 bytes utilizando una velocidad de Tx que varía de: 0.5 Mbps, 0.8 Mbps y 1 Mbps, sin que se pierdan paquetes en la red.

PASO 4: Captura de tráfico con Wireshark.

Capturar tráfico de paquetes en la interfaz s0/1 de R1.

- Captura de paquetes HELLO EIGRP.

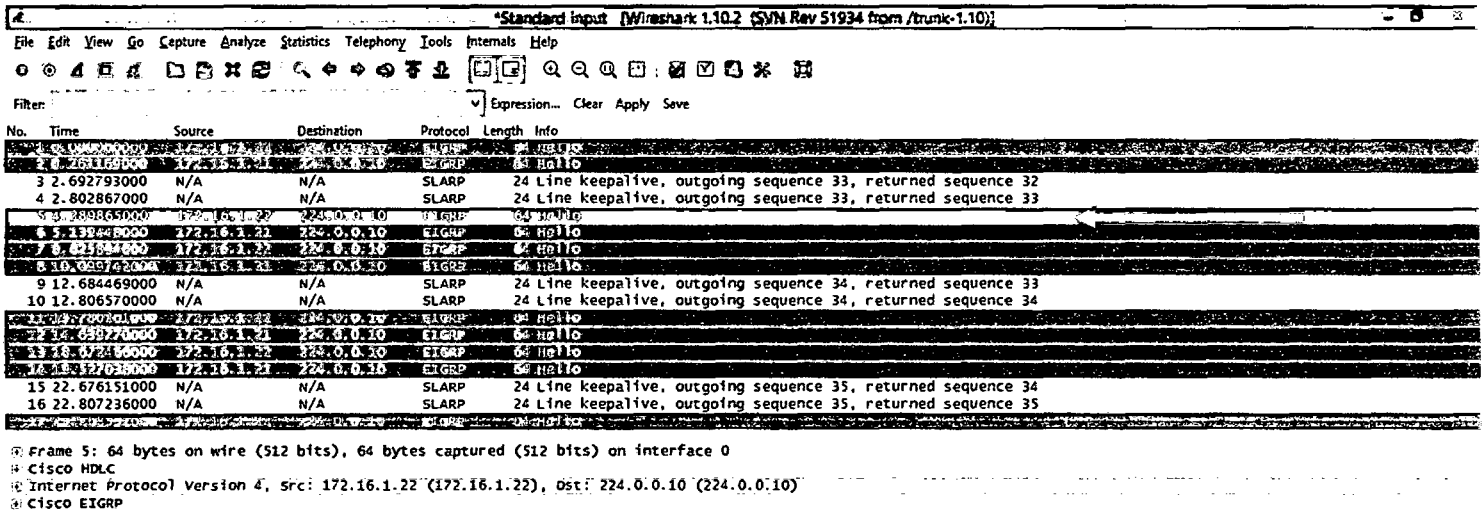


Fig. 4.4.25 Captura de paquete HELLO EIGRP.

Información más detallada sobre el paquete HELLO como parámetros de K1, K3, Checksum, etc.

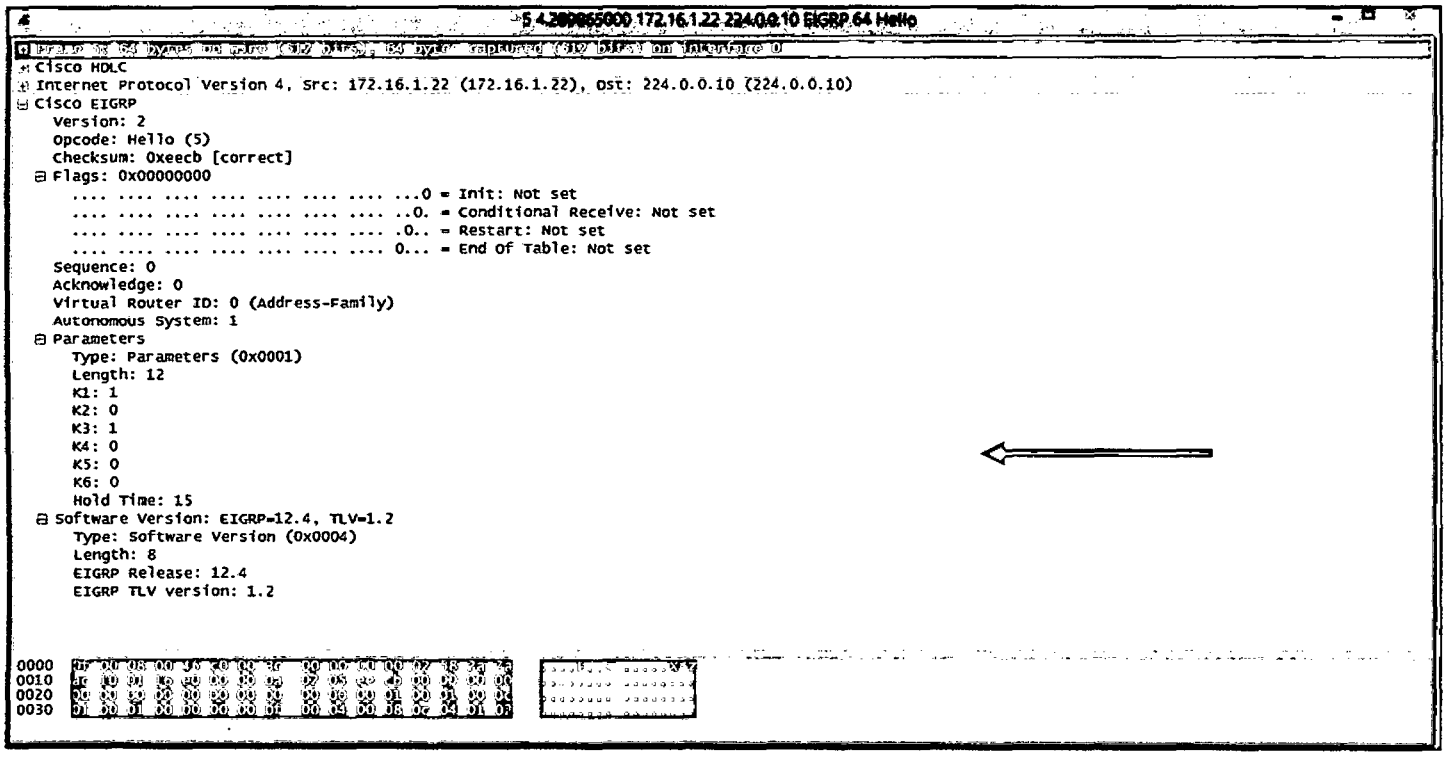


Fig. 4.4.26 Información detallada del paquete HELLO EIGRP.

- Captura de paquetes ICMP.

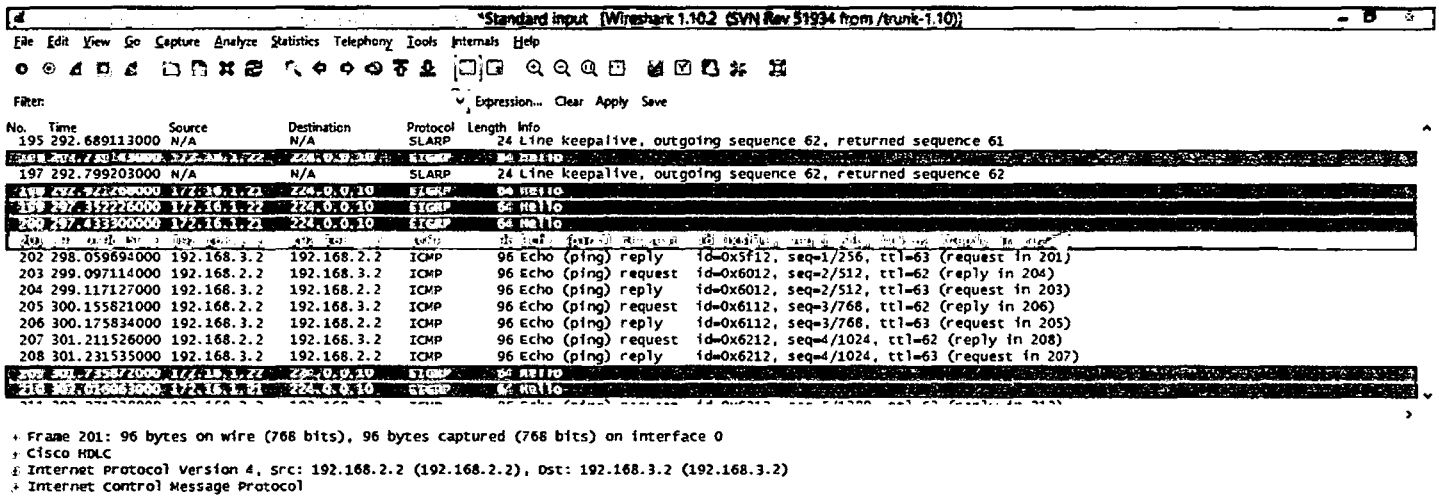


Fig. 4.4.27 Captura de paquetes ICMP con Wireshark.

Información más detallada sobre paquete ICMP:

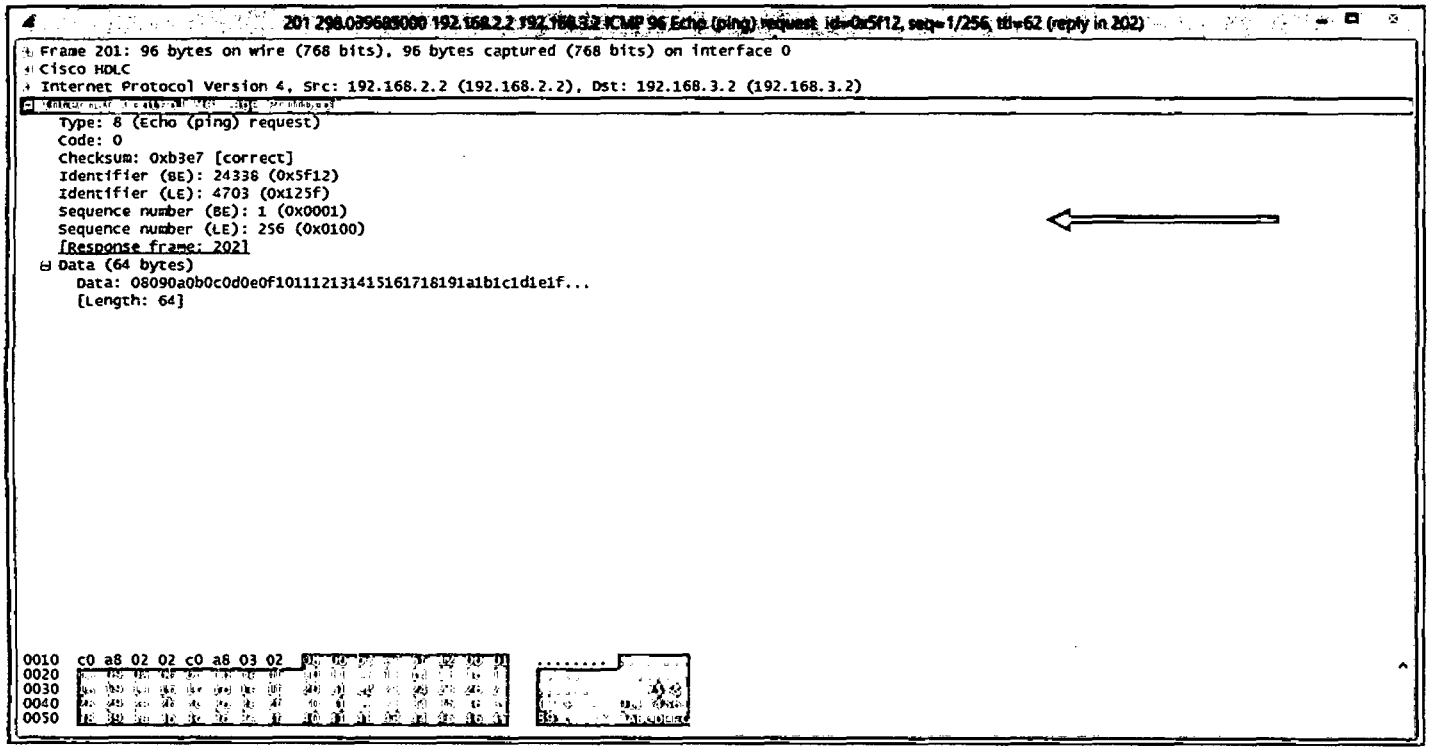


Fig. 4.4.28 Información detallada del paquete ICMP.

- Captura de paquetes CDP (Cisco Discovery Protocol), permite descubrir dispositivos Cisco que estén directamente conectados.

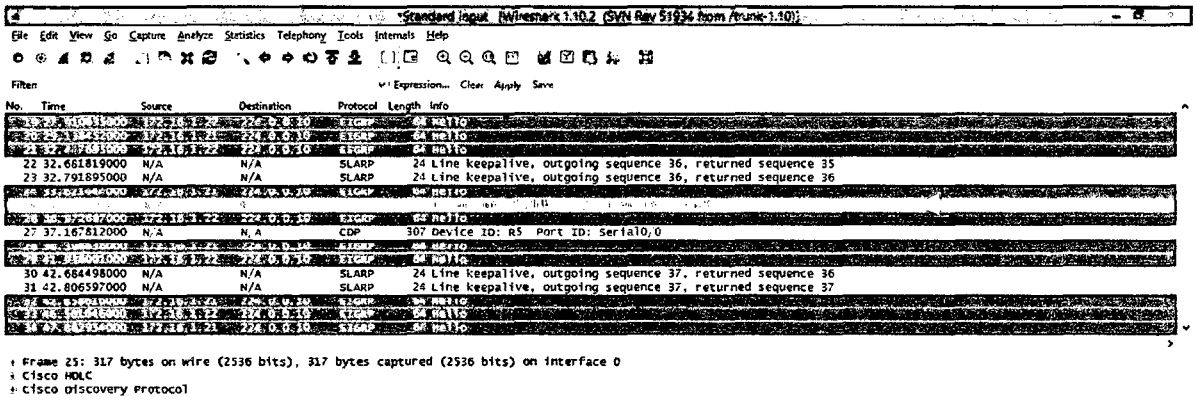


Fig. 4.4.29 Captura de paquete CDP con Wireshark.

Información más detallada sobre el dispositivo descubierto:

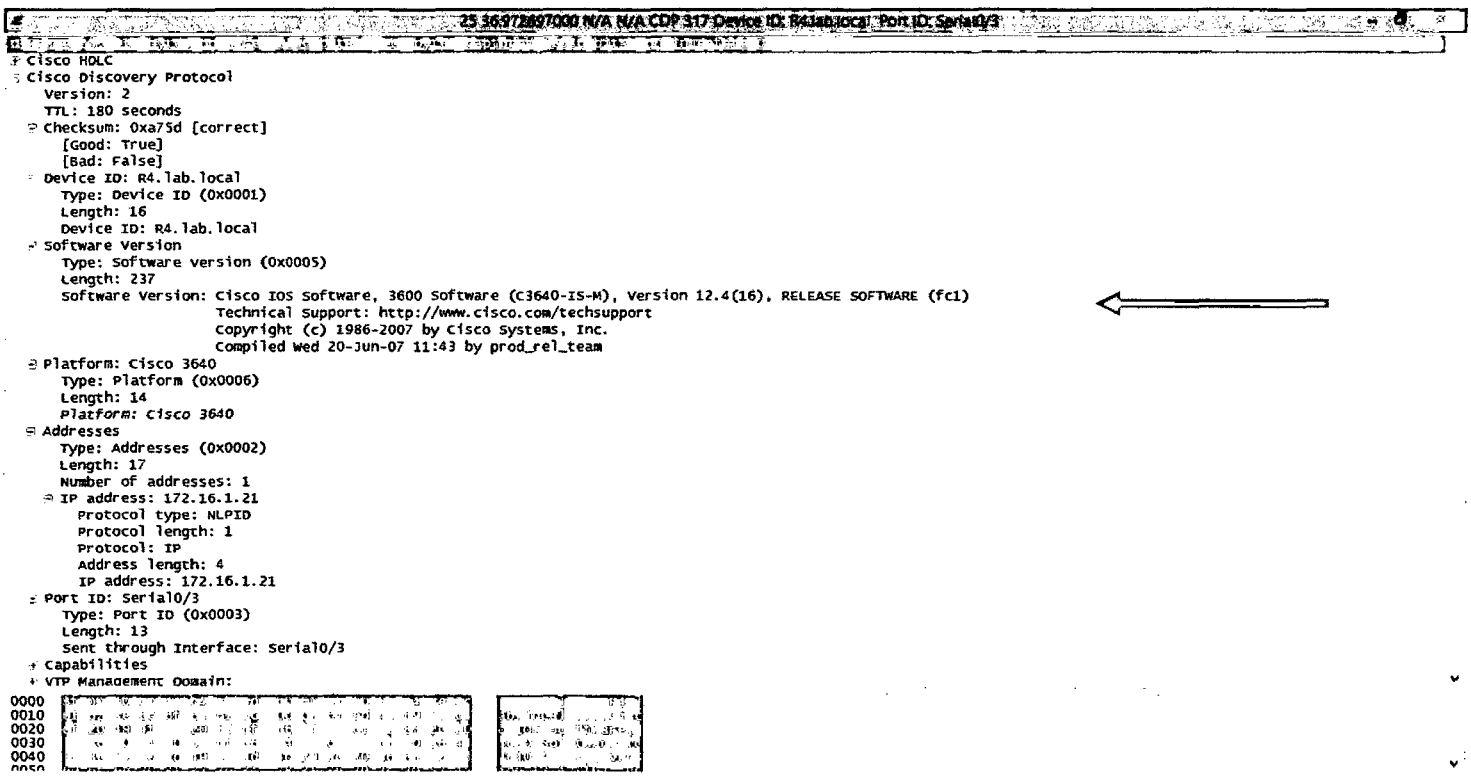


Fig. 4.4.30 Información detallada del paquete CDP.

- Captura de paquetes Telnet

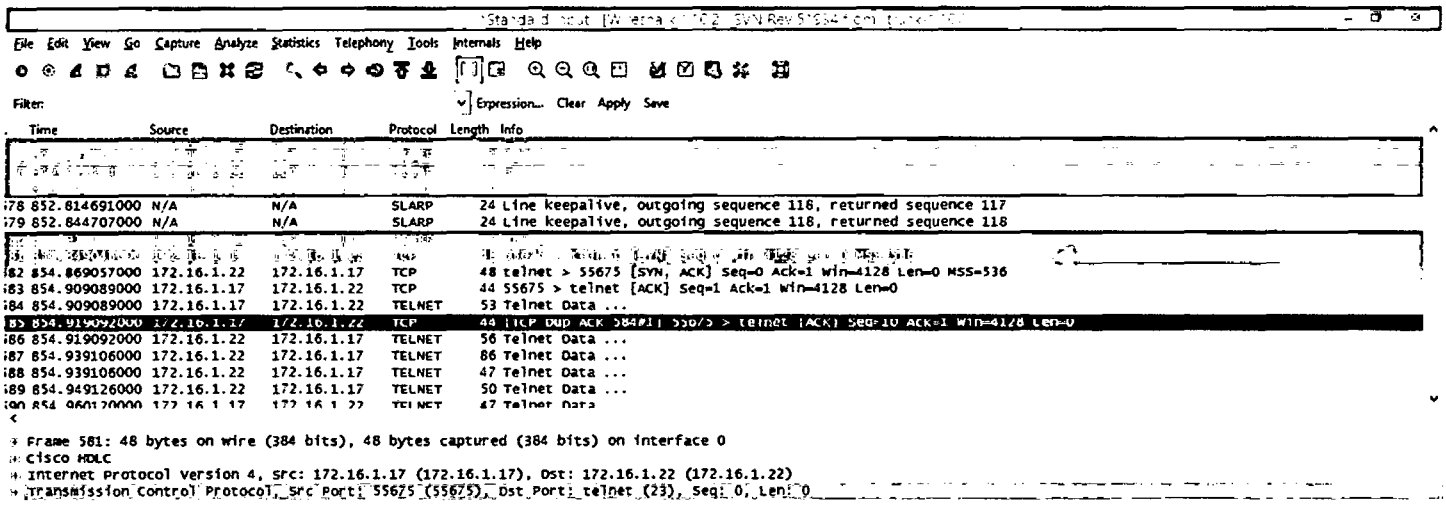


Fig. 4.4.31 Captura de paquete telnet con Wireshark.

- Captura de paquetes Traceroute

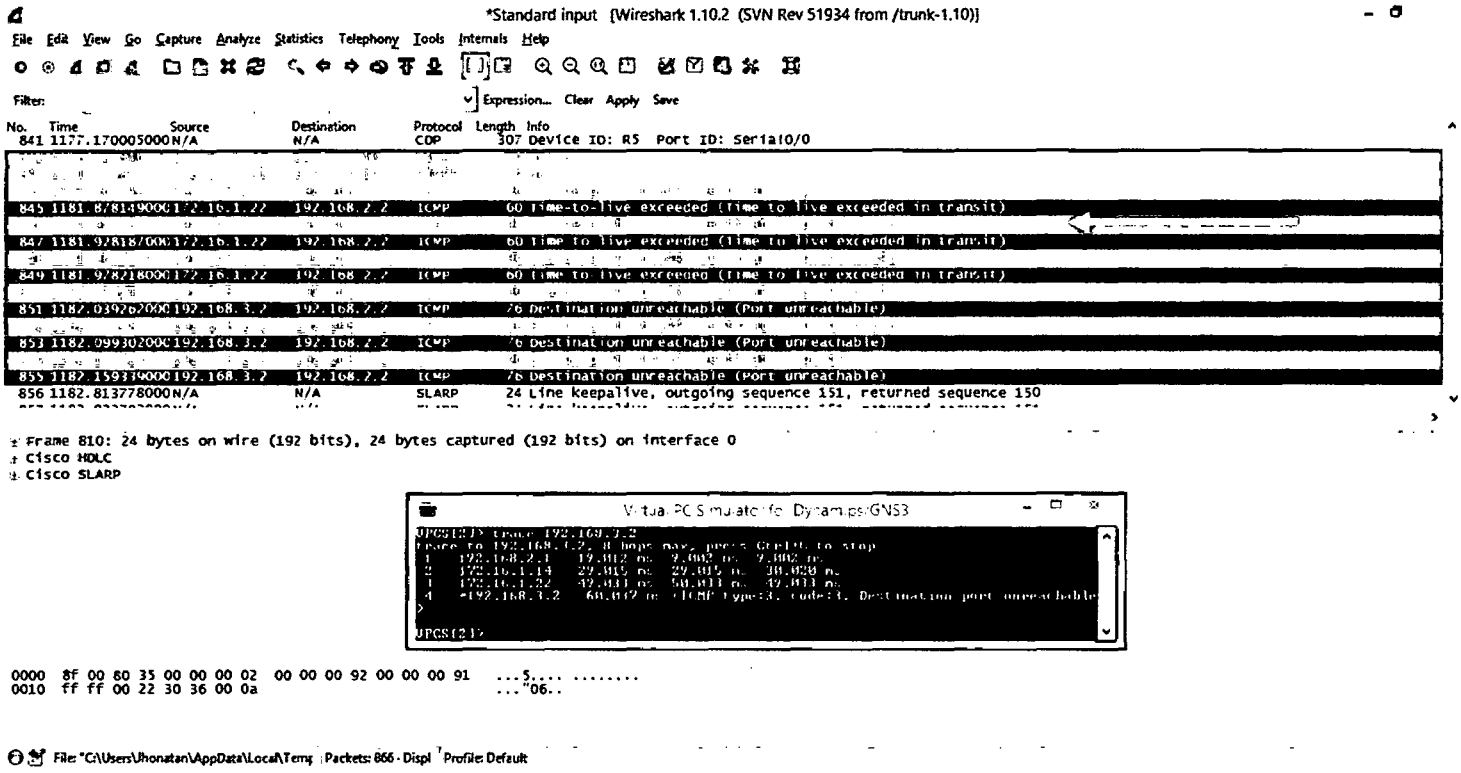


Fig. 4.4.32 Captura de paquetes Traceroute con Wireshark.

LABORATORIO 4.5: CONFIGURACION OSPF

REVISIÓN TEÓRICA: Para la realización de esta práctica se deberá revisar conceptos de enrutamiento OSPF.

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet.
- Configurar el enrutamiento OSPF.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **150.0.0.0/16** para obtener el direccionamiento IP usando VLSM para las interfaces seriales y proporcionar direcciones para las LAN, teniendo los siguientes requisitos:

LAN R4: 20 host.
LAN R5: 30 host.
LAN R6: 10 host.

DIAGRAMA DE TOPOLOGIA

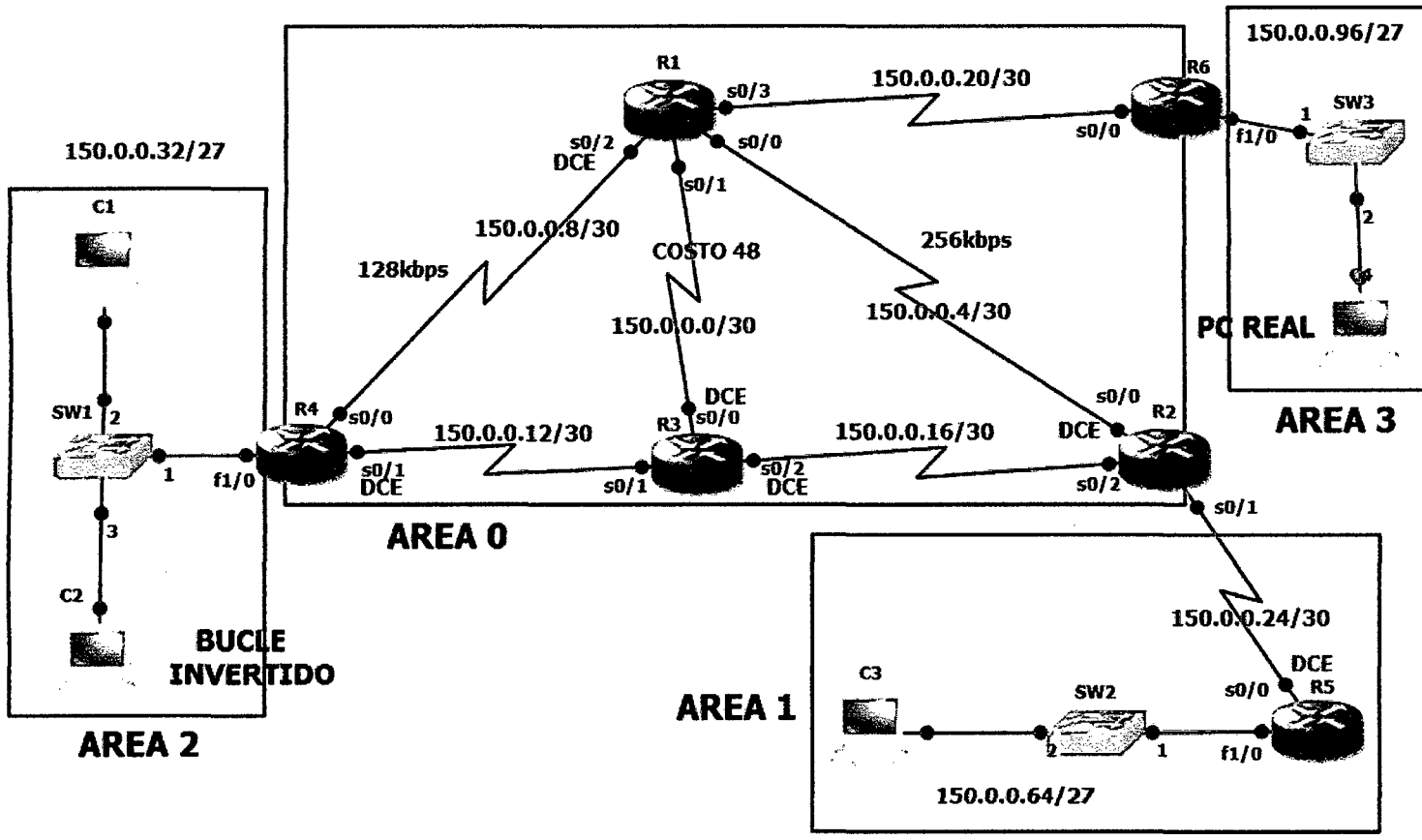


Fig. 4.5.1 Red Virtual en GNS3

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s0/0	150.0.0.5	255.255.255.252	No aplicable
	s0/1	150.0.0.1	255.255.255.252	No aplicable
	s0/2	150.0.0.9	255.255.255.252	No aplicable
	s0/3	150.0.0.21	255.255.255.252	No aplicable
R2	s0/0	150.0.0.6	255.255.255.252	No aplicable
	s0/1	150.0.0.25	255.255.255.252	No aplicable
	s0/2	150.0.0.17	255.255.255.252	No aplicable
R3	s0/0	150.0.0.2	255.255.255.252	No aplicable
	s0/1	150.0.0.13	255.255.255.252	No aplicable
	s0/2	150.0.0.18	255.255.255.252	No aplicable
R4	s0/0	150.0.0.10	255.255.255.252	No aplicable
	s0/1	150.0.0.14	255.255.255.252	No aplicable
	f1/0	150.0.0.33	255.255.255.224	No aplicable
R5	s0/0	150.0.0.26	255.255.255.252	No aplicable
	f1/0	150.0.0.65	255.255.255.224	No aplicable
R6	s0/0	150.0.0.22	255.255.255.252	No aplicable
	f1/0	150.0.0.97	255.255.255.224	No aplicable
C1	VPCS	150.0.0.34	255.255.255.224	150.0.0.33
C2	BUCLE INVERTIDO	150.0.0.35	255.255.255.224	150.0.0.33
C3	VPCS	150.0.0.66	255.255.255.224	150.0.0.65
C4	NIC	150.0.0.98	255.255.255.224	150.0.0.97

Tabla 4.5.1 Direccionamiento IP para las Redes

TAREA 1: MONTAR LA RED EN GNS3

Montar y conectar la red igual a la del Diagrama de topología.

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

Ingrese al modo privilegiado

Router>enable

Aparece el siguiente prompt

Router#

En el modo exec privilegiado, ingrese al modo de configuración global:

Router# **configure terminal**

PASO 1: Establezca la configuración global del nombre de host.

Ingrese el siguiente comando para configurar el nombre del router:

Router(config)#**hostname XXXXXX** (Escribir nombre deseado)

PASO 2: Desactive la búsqueda DNS.

Router(config)# **no ip-domain lookup**

Si escribes algo que no sea un comando de Cisco IOS o cometes un error, el router asume que ha escrito un nombre de dominio y trata de resolver lo que usted escribe, realizando una búsqueda de DNS.

PASO 3: Configure un mensaje para que se muestre al ingresar al router.

Router(config)#**banner motd %** Solo acceso a personal autorizado **%** (Puede escribir cualquier mensaje)

El símbolo % indica el inicio y final del mensaje.

PASO 4: Configure las contraseñas de consola, enable secret y VTY.

Seguir los siguientes pasos:

Router(config)# **line console 0**

Router(config-line)# **password XXXXX** (Escribir contraseña deseada)

Router(config-line)# **login**

Router(config-line)# **exit**

Router(config)# **enable secret XXXXX** (Escribir contraseña deseada)

Router(config)# **line vty 0 4**

Router(config-line)# **password XXXXX** (Escribir contraseña deseada)

Router(config-line)# **login**

Router(config-line)# **exit**

PASO 5: Sincronice los mensajes no solicitados y el resultado de la depuración con el resultado solicitado y los indicadores para las líneas de consola y de terminal virtual.

Router(config)# **line console 0**

Router(config)# **logging synchronous**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **logging synchronous**

Router(config)# **exit**

PASO 6: Configure un tiempo de espera EXEC de 10 minutos.

Router(config)# **line console 0**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

PASO 7: Guardar la configuración.

Router(config)# **copy running-config startup-config**

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET.

Aplique Los siguientes comandos:

R1:

Configuración para una interface serial:

R1(config)# **interface serial 0/0**

R1(config-if)# **description conexion a R2**

R1(config-if)# **ip address 150.0.0.5 255.255.255.252**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

Configuración para una interface fasEthernet:

R1(config)# **interface fasEthernet 1/0**

R1(config-if)# **description conexion a LAN ROUTER FISICO**

R1(config-if)# **ip address 150.0.0.21 255.255.255.252**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

NOTA: Seguir los mismos pasos para las demás routers con sus respectivos parámetros.

TAREA 4: CONFIGURAR OSPF.

PASO 1: Para configurar OSPF, Utilice el siguiente comando.

Router(config)#router ospf [process-id]

Router(config-router)#network [network-adress] [wildcard-mask] area [area-id]

Donde el process-id es un número entre 1 y 65535

R1:

R1(config)# **router ospf 1**

R1(config-router)# **network 150.0.0.0 0.0.0.3 area 0**

R1(config-router)# **network 150.0.0.4 0.0.0.3 area 0**

R1(config-router)# **network 150.0.0.8 0.0.0.3 area 0**

R1(config-router)# **network 150.0.0.20 0.0.0.3 area 0**

R1(config-router)# **exit**

R4:

R4(config)# **router ospf 1**

R4(config-router)# **network 150.0.0.8 0.0.0.3 area 0**

R4(config-router)# **network 150.0.0.12 0.0.0.3 area 0**

R4(config-router)# **network 150.0.0.32 0.0.0.31 area 0**

R4(config-router)# **exit**

NOTA: Seguir la misma configuración para los demás routers con sus respectivas redes.

PASO 2: Modificar bandwidth.

R1:

R1(config)# **interface serial 0/0**

R1(config-if)# **bandwidth 256**

R1(config-if)# **exit**

R1(config)# **interface serial 0/2**

R1(config-if)# **bandwidth 128**

R1(config-if)# **exit**

PASO 3: Modificar el costo del enlace.

R1:

R1(config)# **interface serial 0/1**

R1(config-if)# **ip ospf cost 48**

R1(config-if)# **end**

TAREA 5: CONFIGURAR LOS EQUIPOS DE HOST.

VPCS

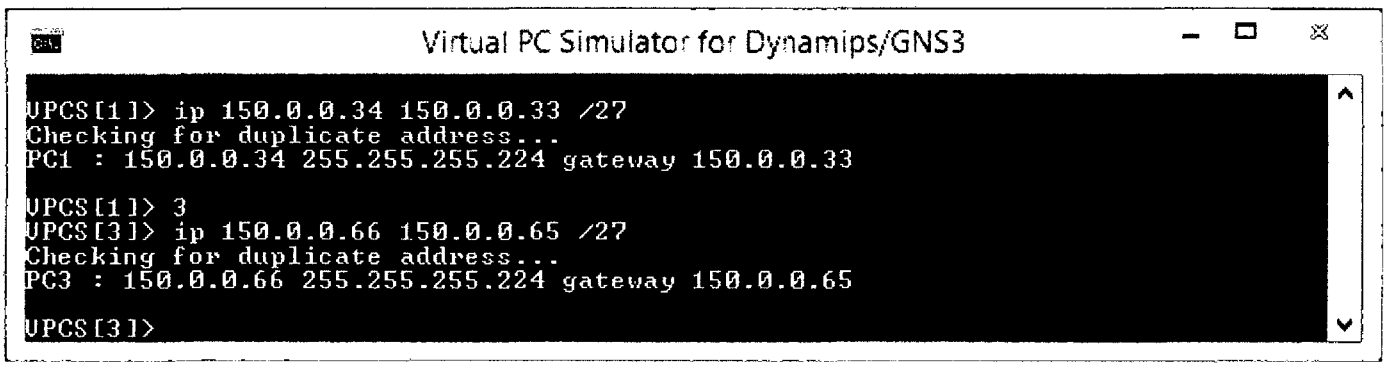


Fig. 4.5.2 Configuración de IP para VPCS.

PC REAL

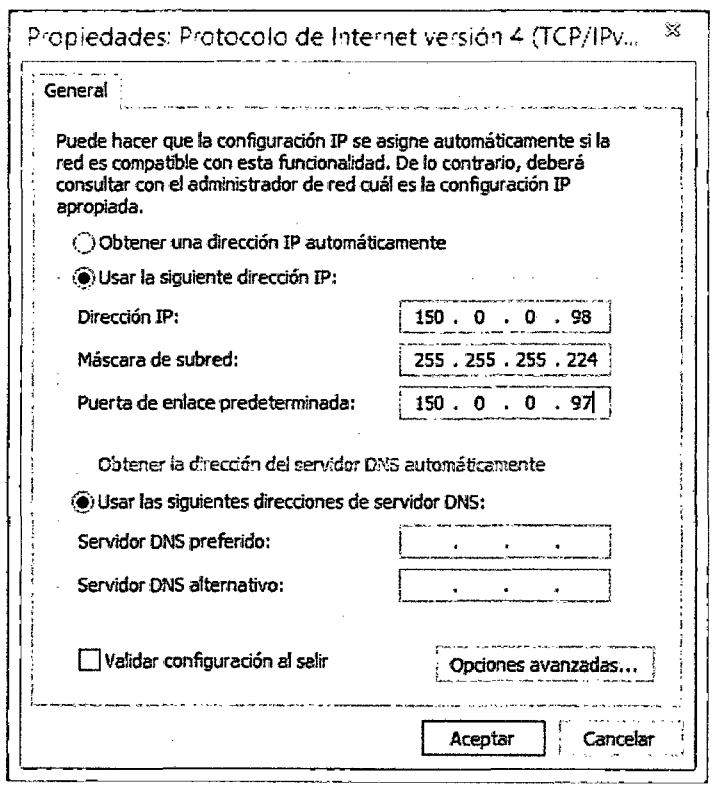


Fig. 4.5.3 Configuración de IP para PC REAL.

NOTA: Configurar los demás host.

TAREA 6: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

PASO 1: Verificar configuraciones.

R1#show ip ospf interface brief

Nos muestra la interfaz a través del cual el router está conectado con el vecino, el área, el costo, el número routers vecinos adyacentes, etc.

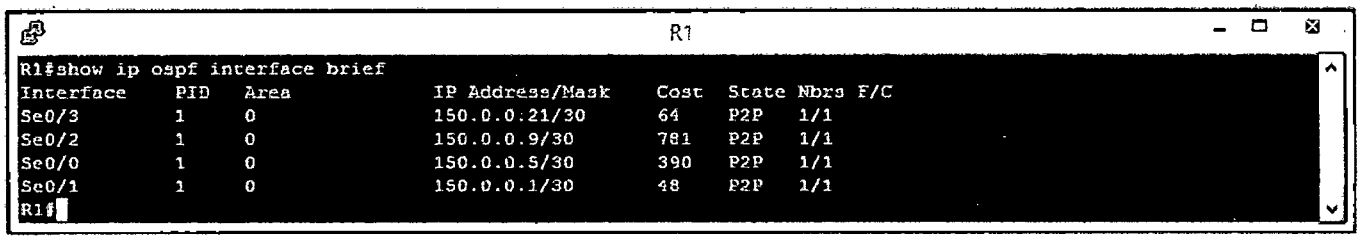


Fig. 4.5.4 Tabla ip ospf interface brief.

R1#show ip protocols

Muestra los parámetros y estado actual del protocolo de enrutamiento activo.

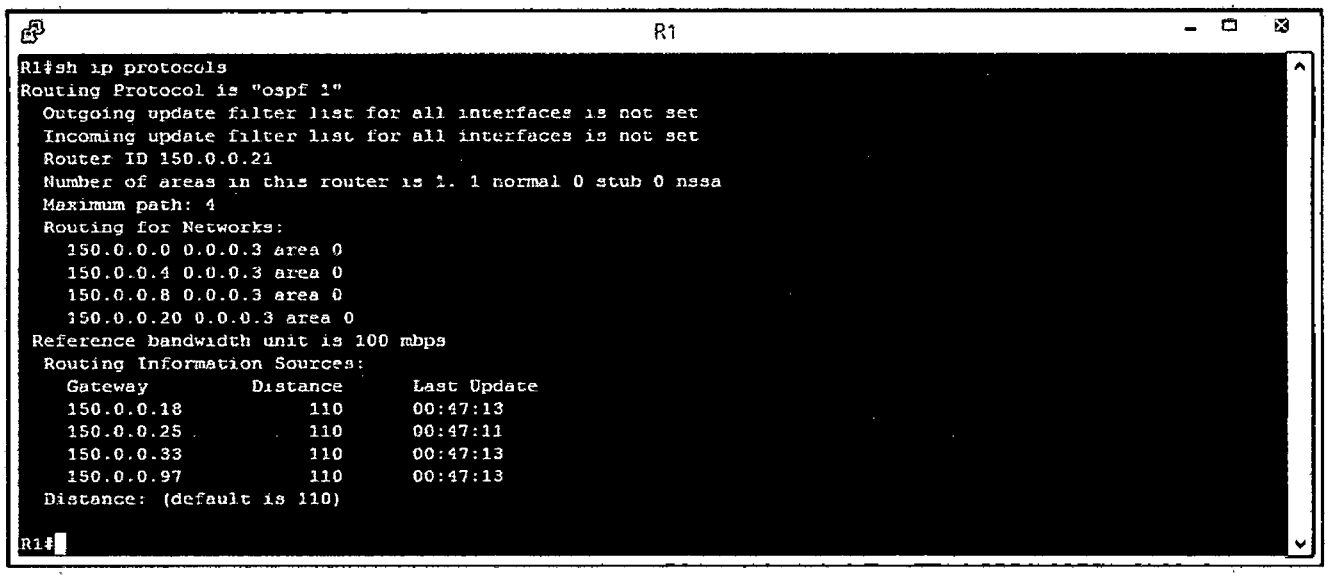


Fig. 4.5.5 Tabla ip protocols.

R1#show ip interface brief

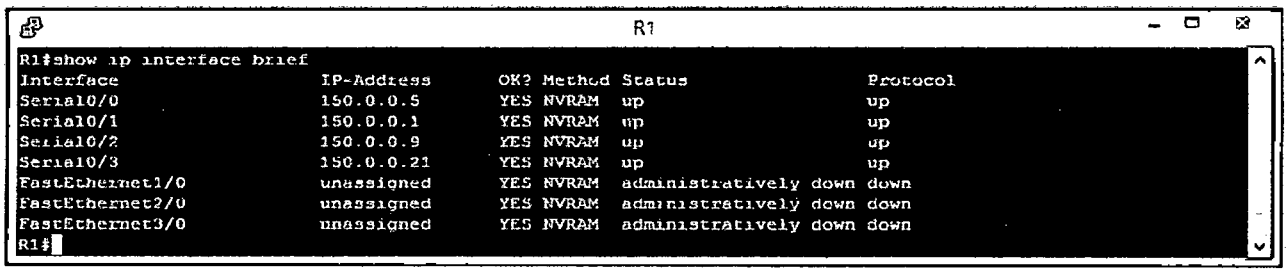


Fig. 4.5.6 Tabla ip interface brief.

R1#show ip route

Muestra el contenido de la tabla de enrutamiento IP.

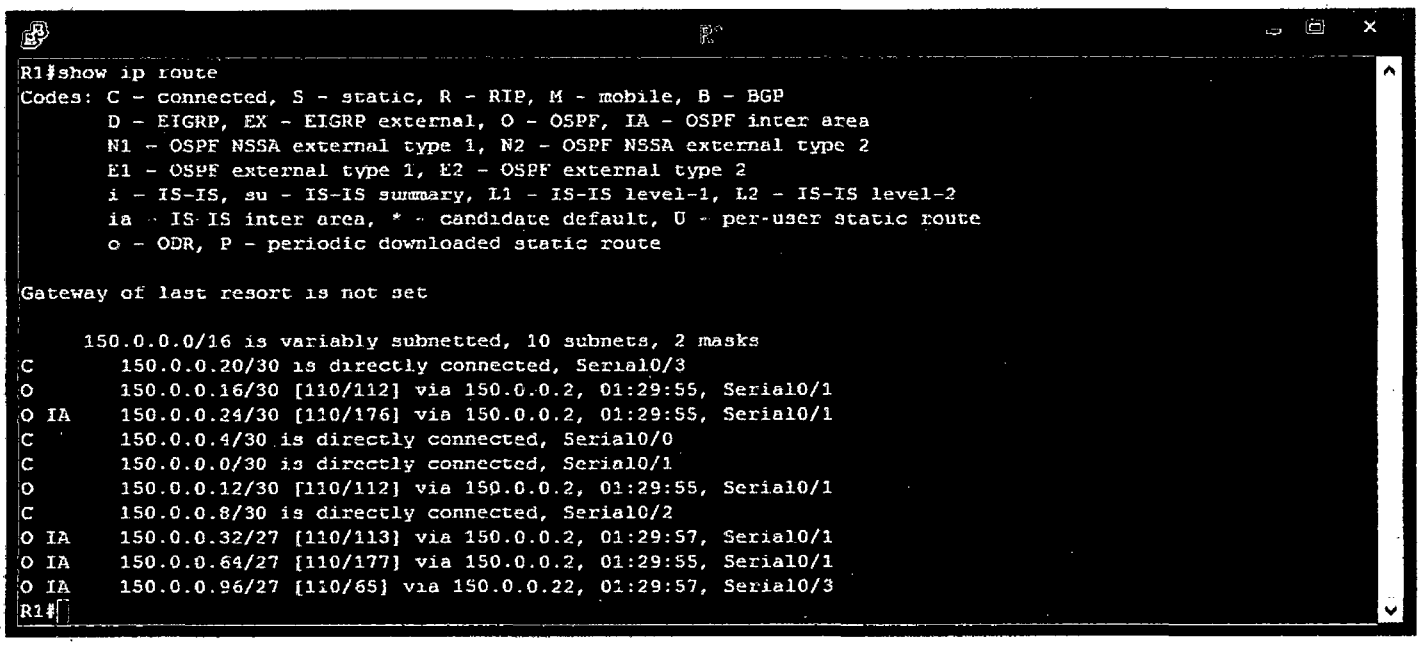


Fig. 4.5.7 Tabla de enrutamiento de R1.

R1#show ip ospf database

Nos muestra el ID de entrada, area-id, checksum, ID de la ruta publicada (ADV Router), etc.

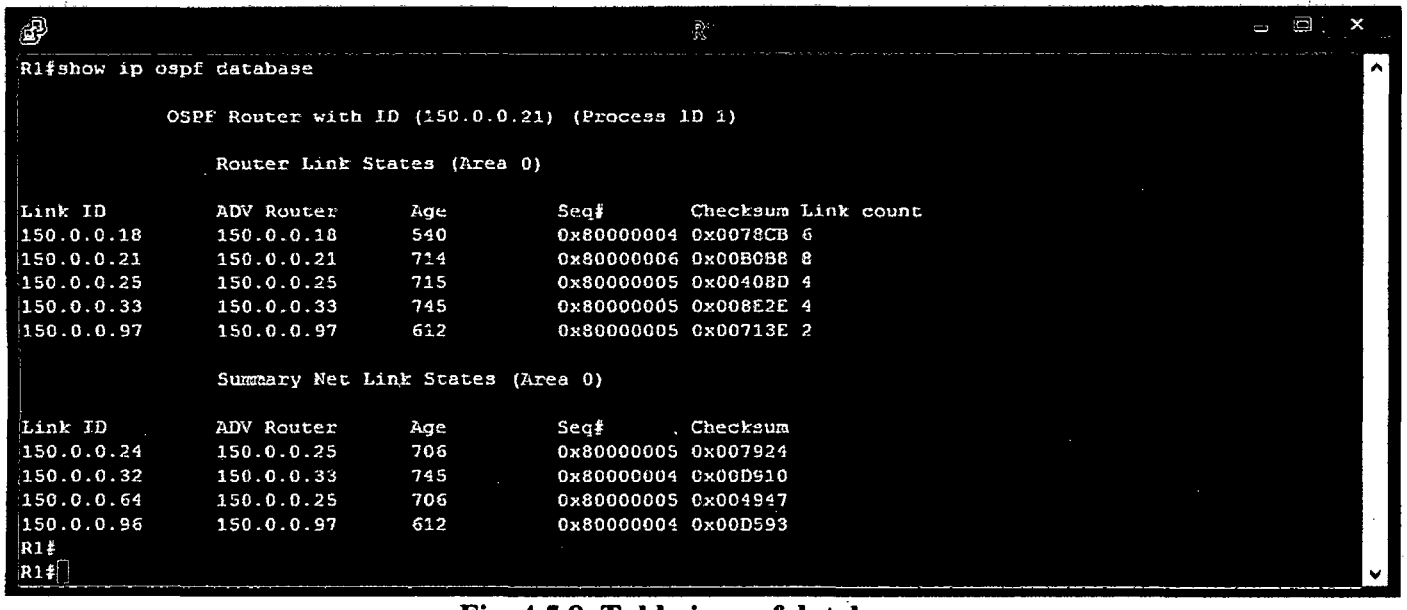


Fig. 4.5.8 Tabla ip ospf database.

PASO 2: Utilice el comando ping para probar la conectividad entre los routers que no están directamente conectados y también la conectividad entre host.

PING ENTRE ROUTERS

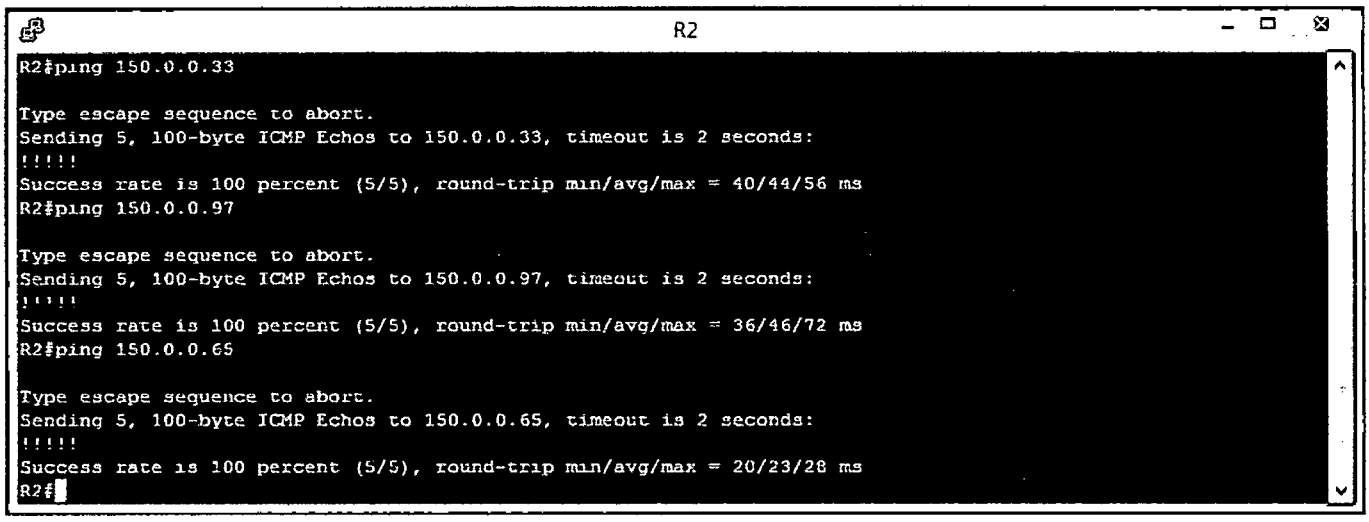


Fig. 4.5.9 Prueba de conectividad entre routers.

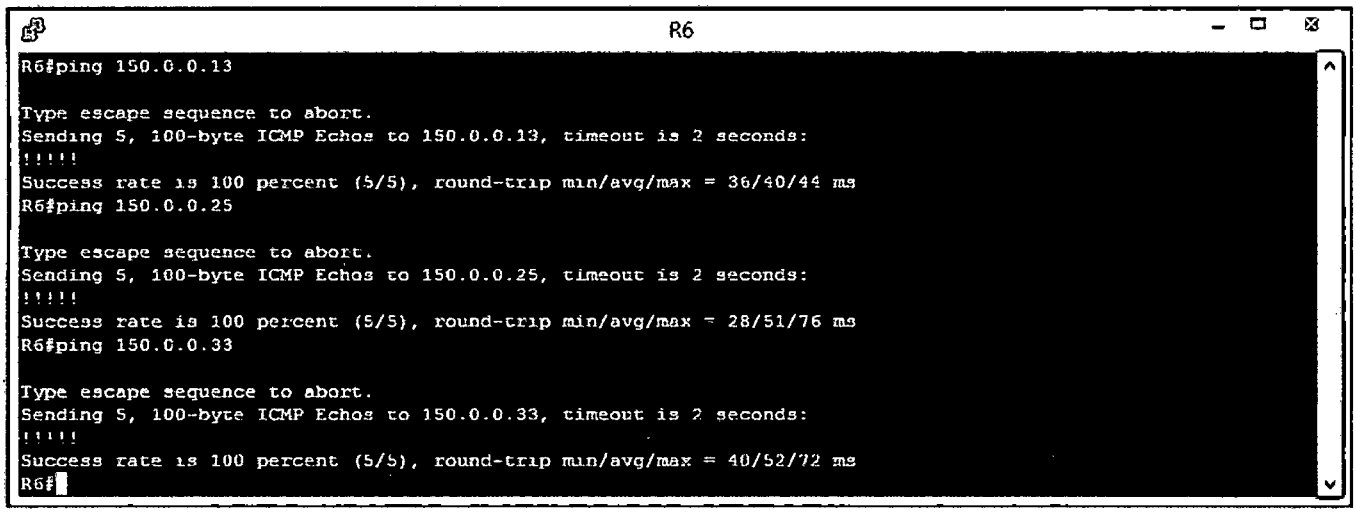


Fig. 4.5.10 Prueba de conectividad entre routers.

PING ENTRE HOST

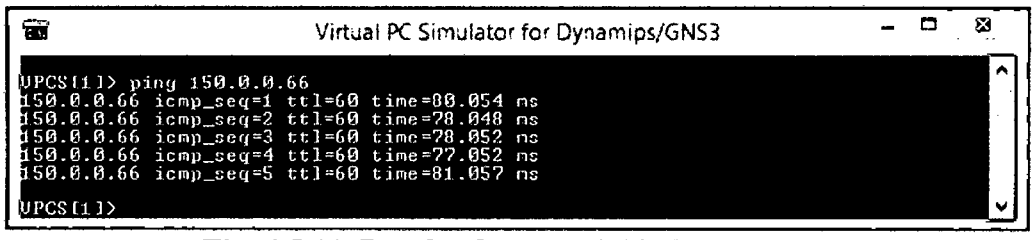


Fig. 4.5.11 Prueba de conectividad entre host.

NOTA: Realizar las pruebas faltantes.

TAREA 7: ANALIS DEL TRAFICO DE PAQUETES

PASO 1: Medición de la Latencia

Para la medición de la latencia se realizó 10 muestras sucesivas de 100 ping desde el C2 (Bucle invertido) hacia la PC REAL considerando un tamaño de trama de 64, 512 y 1518 bytes como se especifica en el RFC 2544.

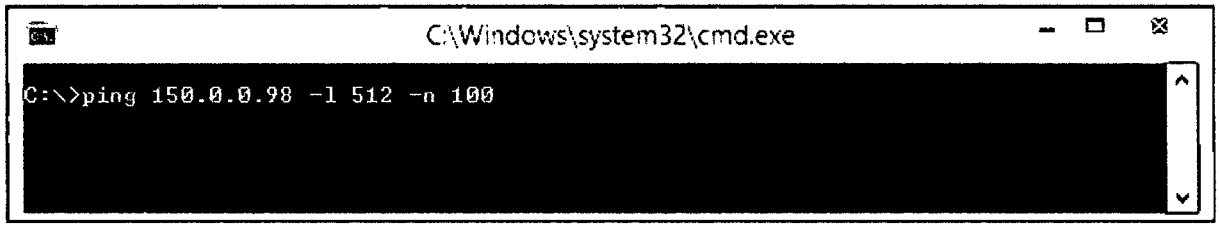


Fig. 4.5.12 Forma de medición de la latencia.

En la Figura 4.5.12 se puede observar el envío de 100 ping con una trama de 512 hacia la dirección 150.0.0.98

En las Tablas posteriores se detallan los valores de la Latencia que se ha obtenido una vez realizadas todas las muestras.

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	**97**	**98**	**96**	**97**	**95**	**97**	**95**	**99**	**95**	**98**	**96.7**
Tiempo Máximo (ms)	**118**	**110**	**118**	**108**	**111**	**107**	**119**	**108**	**112**	**108**	**111.9**
Tiempo Promedio (ms)	**105**	**102**	**104**	**101**	**104**	**101**	**102**	**103**	**102**	**103**	**102.7**

Tabla 4.5.2 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	512										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	95	96	97	99	100	98	94	96	98	96	96.9
Tiempo Máximo (ms)	112	118	113	111	115	113	127	113	111	108	114.1
Tiempo Promedio (ms)	104	103	101	108	106	105	103	104	107	104	104.5

Tabla 4.5.3 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1518										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	125	126	122	118	113	120	126	126	121	126	122.3
Tiempo Máximo (ms)	162	144	160	141	138	141	142	141	139	142	145
Tiempo Promedio (ms)	135	135	136	133	132	132	131	134	130	137	133.5

Tabla 4.5.4 Datos obtenidos para una trama de 1518 bytes.

LATENCIA			
Tamaño de Trama (bytes)	64	512	1518
Tiempo Mínimo (ms)	96.7	96.9	122.3
Tiempo Máximo (ms)	111.9	114.1	145
Tiempo Promedio (ms)	102.7	104.5	133.5

Tabla 4.5.5 Comparación de datos obtenidos de las diferentes tramas.

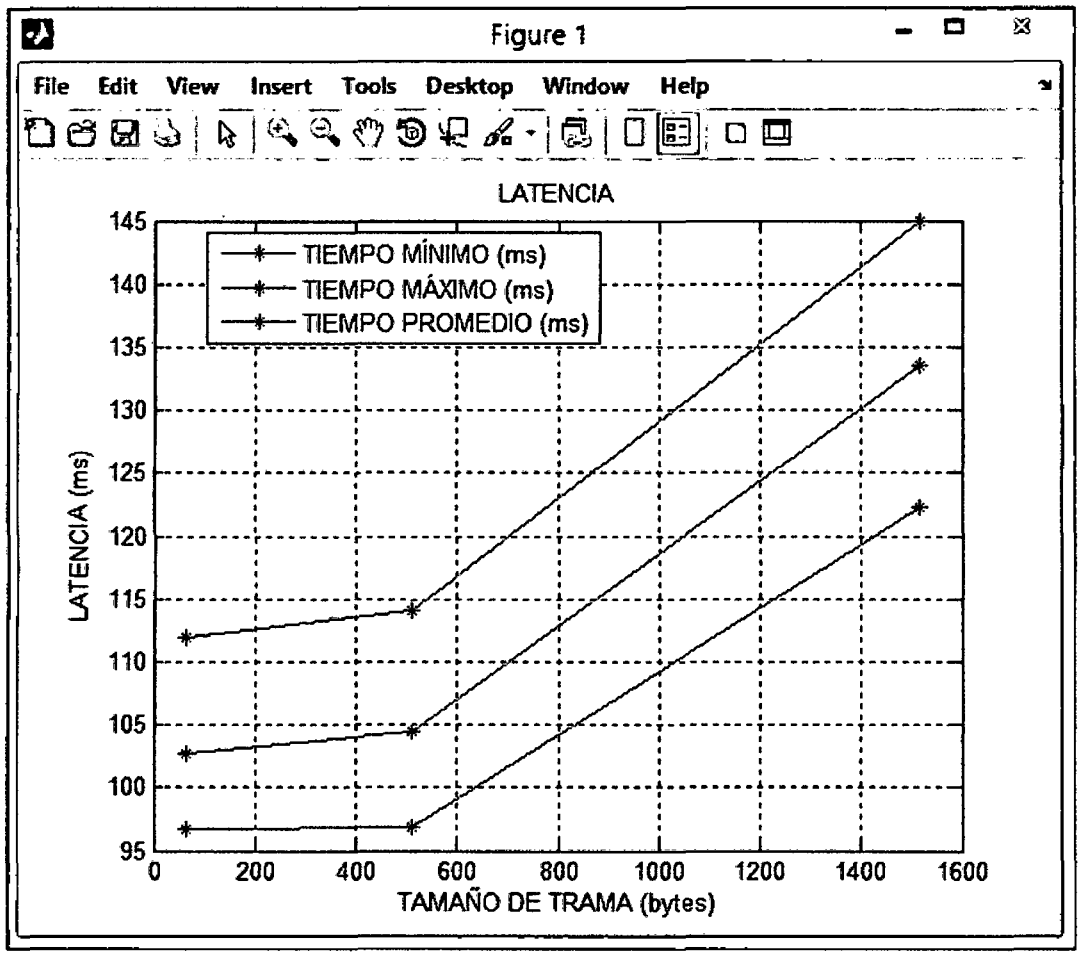


Fig. 4.5.13 Datos representados gráficamente de la variación de la latencia.

De acuerdo con los datos obtenidos, se puede observar claramente que los valores mínimo (color azul), máximo (color rojo) y promedio (color verde) de la latencia de la red se incrementan conforme se envía una trama de longitud mayor, en este caso con la trama de 1518 bytes se obtiene una latencia promedio de 133.5 ms a diferencia de una trama de 64 bytes con 102.7 ms.

PASO 2: Medición del Throughput

Para la medición del Throughput y Jitter se envió una cantidad de tramas a velocidades diferentes durante 20 segundos, hasta encontrar la máxima cantidad de tramas recibidas sin que se produzcan perdidas de las mismas en el router y PC REAL. Como se utilizó Jperf el cliente será el encargado de enviar los paquetes y el servidor los recibirá, indicando la cantidad de paquetes que llegaron correctamente considerando un tamaño del paquete UDP de 750, 1125, 1500 y 1470 (default) bytes, tal como se especifica en el RFC 768.

Configuración del Jperf como servidor con UDP Packet Size 1125 Bytes.

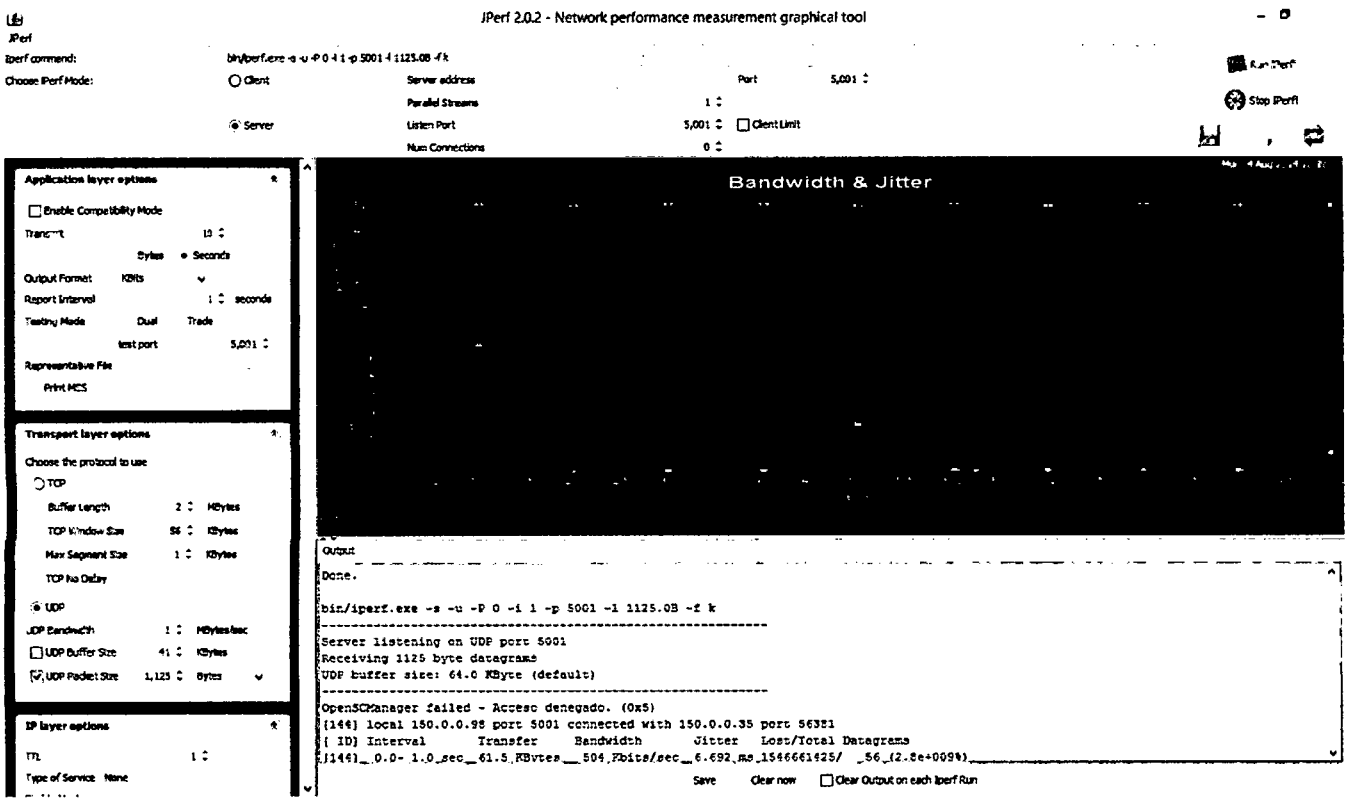


Fig. 4.5.14 Gráfica de Bandwidth y Jitter.

```
bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -l 1125.0B -f k
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1125 byte datagrams
UDP buffer size: 64.0 KByte (default)
------------------------------------------------------------
OpenSCManager failed - Acceso denegado. (0x5)
[144] local 150.0.0.98 port 5001 connected with 150.0.0.35 port 56381
[ ID] Interval       Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[144]  0.0- 1.0 sec  61.5 KBytes   504 Kbits/sec  6.692 ms 1546661425/   56 (2.8e+009%)
[144]  1.0- 2.0 sec  60.4 KBytes   495 Kbits/sec  0.195 ms    0/   55 (0%)
[144]  2.0- 3.0 sec  61.5 KBytes   504 Kbits/sec  0.013 ms    0/   56 (0%)
[144]  3.0- 4.0 sec  61.5 KBytes   504 Kbits/sec  0.002 ms    0/   56 (0%)
[144]  4.0- 5.0 sec  60.4 KBytes   495 Kbits/sec  2.483 ms    0/   55 (0%)
[144]  5.0- 6.0 sec  61.5 KBytes   504 Kbits/sec  0.073 ms    0/   56 (0%)
[144]  6.0- 7.0 sec  60.4 KBytes   495 Kbits/sec  0.005 ms    0/   55 (0%)
[144]  7.0- 8.0 sec  61.5 KBytes   504 Kbits/sec  0.002 ms    0/   56 (0%)
[144]  8.0- 9.0 sec  60.4 KBytes   495 Kbits/sec  0.002 ms    0/   55 (0%)
[144]  9.0-10.0 sec  60.4 KBytes   495 Kbits/sec  0.982 ms    0/   55 (0%)
[144]  0.0-10.0 sec   611 KBytes   500 Kbits/sec  0.920 ms    0/  556 (0%)
```

Fig. 4.5.15 Resultados al medir como servidor.

Configuración del Jperf como cliente con UDP Bandwidth 500 Kbps y UDP Packet Size de 1125 Bytes.

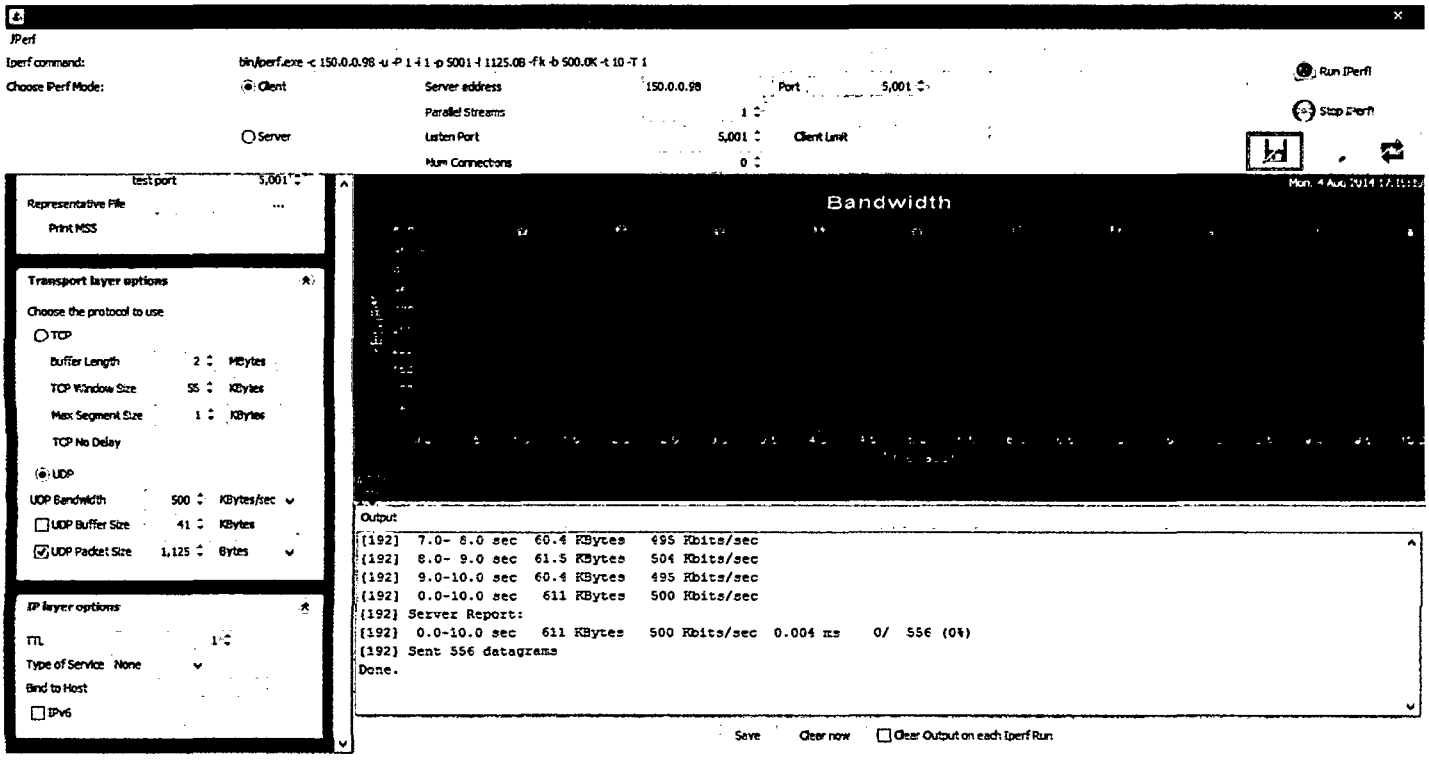


Fig. 4.5.16 Resultados del Jperf como Cliente.

En las siguientes Tablas se detalla los valores del Throughput obtenidos una vez realizada todas las muestras.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**0.5**	**0.5**	**0.5**
Velocidad de Rx (Mbps)	**0.5**	**0.5**	**0.5**
Tramas Transmitidas	**834**	**556**	**418**
Tramas Recibidas	**834**	**556**	**418**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**83.4**	**55.6**	**41.8**

Tabla 4.5.6 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**0.1**	**0.5**	**0.8**
Velocidad de Rx (Mbps)	**0.1**	**0.5**	**0.8**
Tramas Transmitidas	**86**	**426**	**681**
Tramas Recibidas	**86**	**426**	**681**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**8.6**	**42.6**	**68.1**

Tabla 4.5.7 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

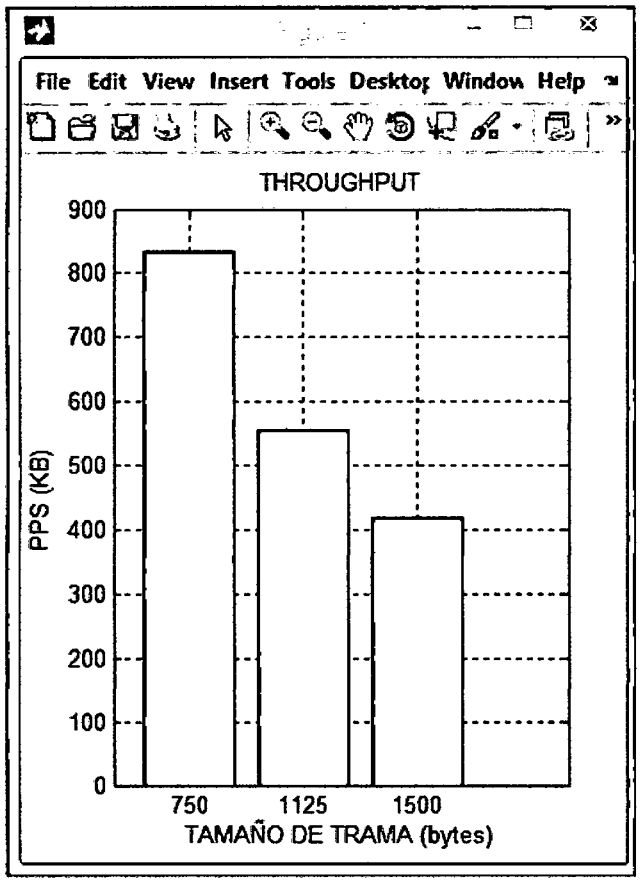


Fig. 4.5.17 PPS vs. Tamaño de Trama.

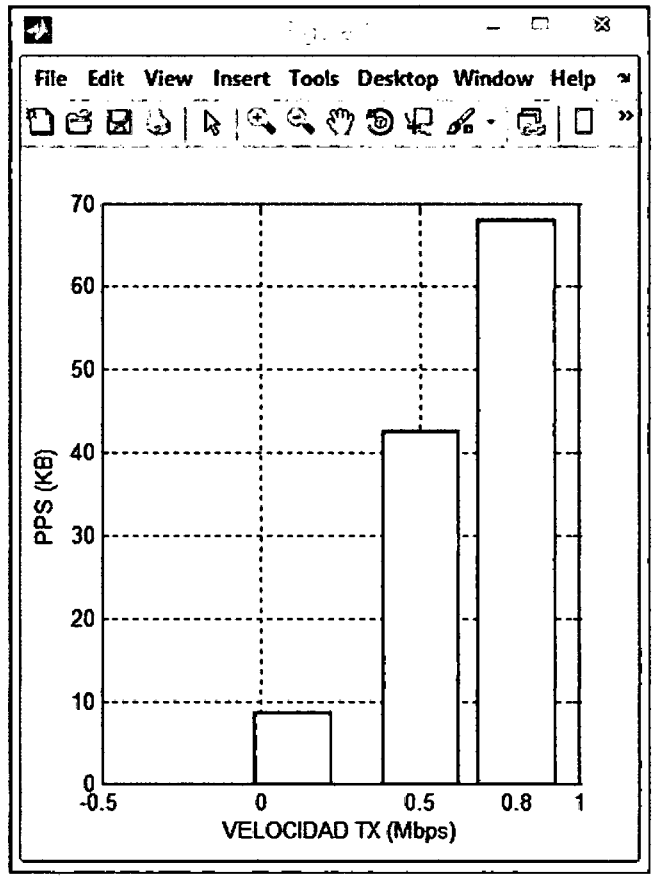


Fig. 4.5.18 PPS vs. Velocidad Tx.

En la figura 4.5.16, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 750 bytes, 1125 bytes y 1500 bytes los cuales han utilizado una velocidad de Tx constante de 0.5 Mbps, en la gráfica se puede observar claramente que al enviar una trama de 750 bytes se envía 834 pps, con una trama de 1125 se envía 556 pps y con una trama de 1500 se envía 418 pps.

Mientras en la figura 4.5.17, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 1470 bytes los cuales han utilizado una velocidad de Tx variada de: 0.1 Mbps, 0.5 Mbps y 0.8 Mbps, sin que se produzcan perdidas en el envío, como los datos que se muestran en la tabla 4.5.7.

PASO 3: Medición del Jitter

Para la medición se envió datos UDP de longitud variable a velocidades diferentes de Throughput obtenida anteriormente durante 20 segundos. Como se utilizó anteriormente Jperf el cliente será el encargado de enviar los datos y el servidor los recibirá, indicando los valores de Jitter obtenidos durante la transmisión de los datos.

Configuración del Jperf como servidor con UDP Packet Size por defecto.

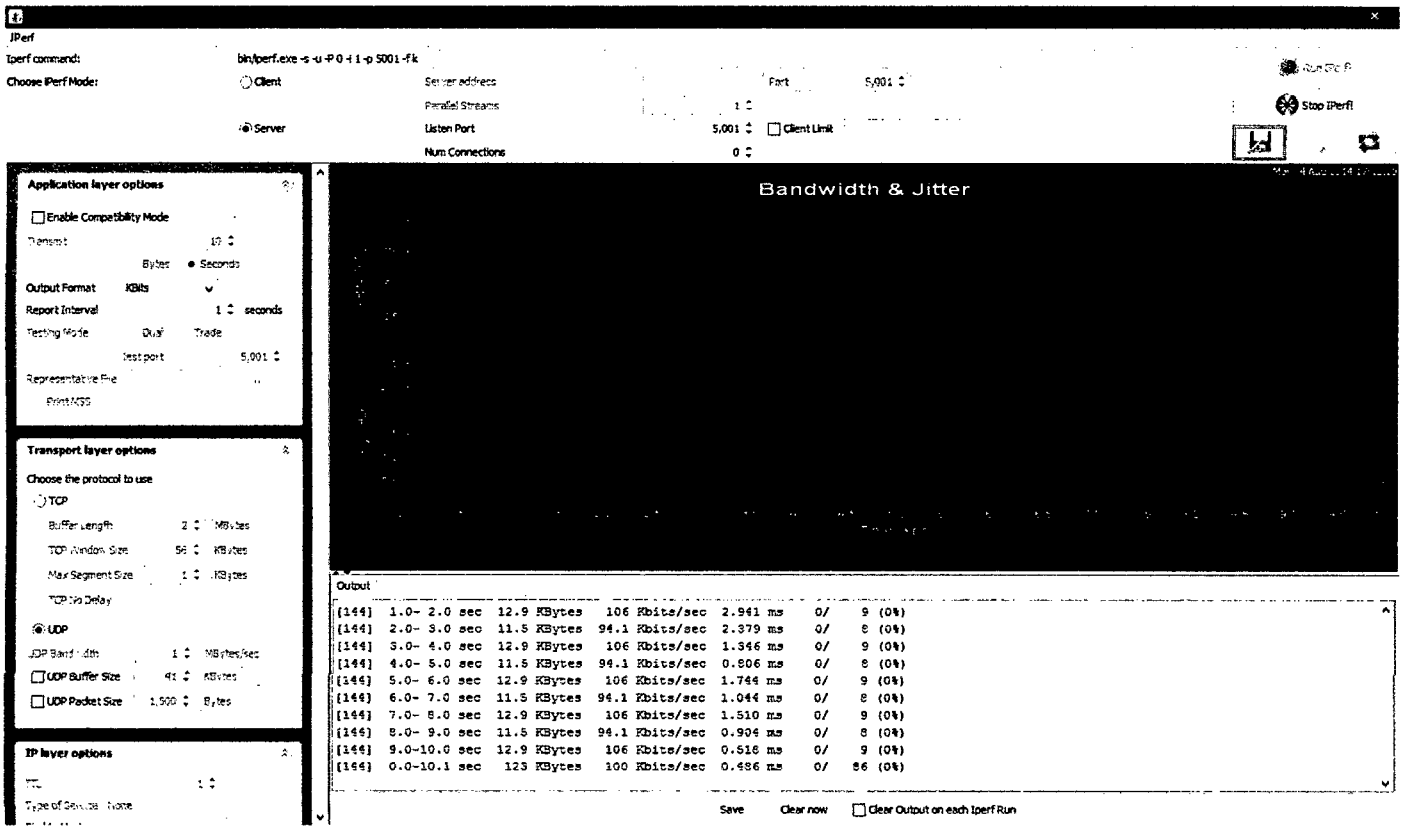


Fig. 4.5.19 Gráfica de Bandwidth y Jitter.

```
bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -f k
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 64.0 KByte (default)
------------------------------------------------------------
OpenSCManager failed - Acceso denegado. (0x5)
[144] local 150.0.0.98 port 5001 connected with 150.0.0.35 port 64856
[ ID] Interval       Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[144]  0.0- 1.0 sec  11.5 KBytes  94.1 Kbits/sec  0.003 ms 1546661425/    8 (1.9e+010%)
[144]  1.0- 2.0 sec  12.9 KBytes   106 Kbits/sec  2.941 ms    0/    9 (0%)
[144]  2.0- 3.0 sec  11.5 KBytes  94.1 Kbits/sec  2.379 ms    0/    8 (0%)
[144]  3.0- 4.0 sec  12.9 KBytes   106 Kbits/sec  1.346 ms    0/    9 (0%)
[144]  4.0- 5.0 sec  11.5 KBytes  94.1 Kbits/sec  0.806 ms    0/    8 (0%)
[144]  5.0- 6.0 sec  12.9 KBytes   106 Kbits/sec  1.744 ms    0/    9 (0%)
[144]  6.0- 7.0 sec  11.5 KBytes  94.1 Kbits/sec  1.044 ms    0/    8 (0%)
[144]  7.0- 8.0 sec  12.9 KBytes   106 Kbits/sec  1.510 ms    0/    9 (0%)
[144]  8.0- 9.0 sec  11.5 KBytes  94.1 Kbits/sec  0.904 ms    0/    8 (0%)
[144]  9.0-10.0 sec  12.9 KBytes   106 Kbits/sec  0.518 ms    0/    9 (0%)
[144]  0.0-10.1 sec   123 KBytes   100 Kbits/sec  0.486 ms    0/   86 (0%)
```

Fig. 4.5.20 Resultados al medir como servidor.

En las siguientes Tablas se detalla los valores del Jitter obtenidos una vez realizada todas las muestras.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**0.5**	**0.5**	**0.5**
Velocidad de Rx (Mbps)	**0.5**	**0.5**	**0.5**
Tramas Transmitidas	**834**	**556**	**418**
Tramas Recibidas	**834**	**556**	**418**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**0.433**	**0.920**	**1.036**

Tabla 4.5.8 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**0.1**	**0.5**	**0.8**
Velocidad de Rx (Mbps)	**0.1**	**0.5**	**0.8**
Tramas Transmitidas	**86**	**426**	**681**
Tramas Recibidas	**86**	**426**	**681**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**0.486**	**0.876**	**1.853**

Tabla 4.5.9 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

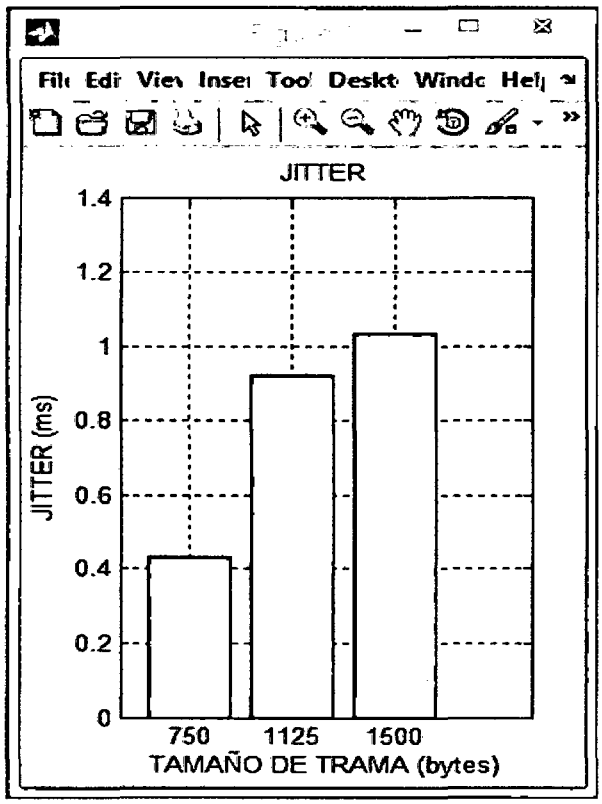


Fig. 4.5.21 Jitter vs. Tamaño de Trama

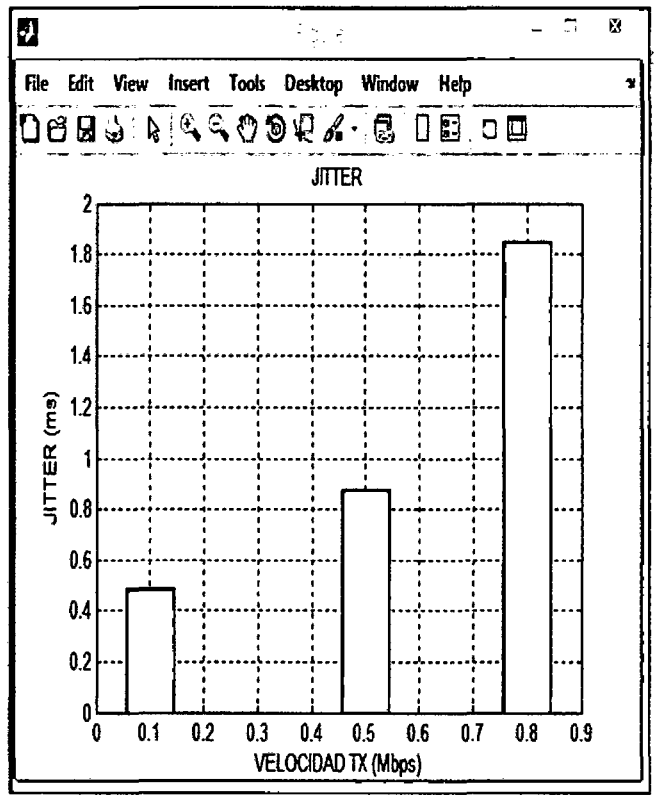


Fig. 4.5.22 Jitter vs. Velocidad Tx

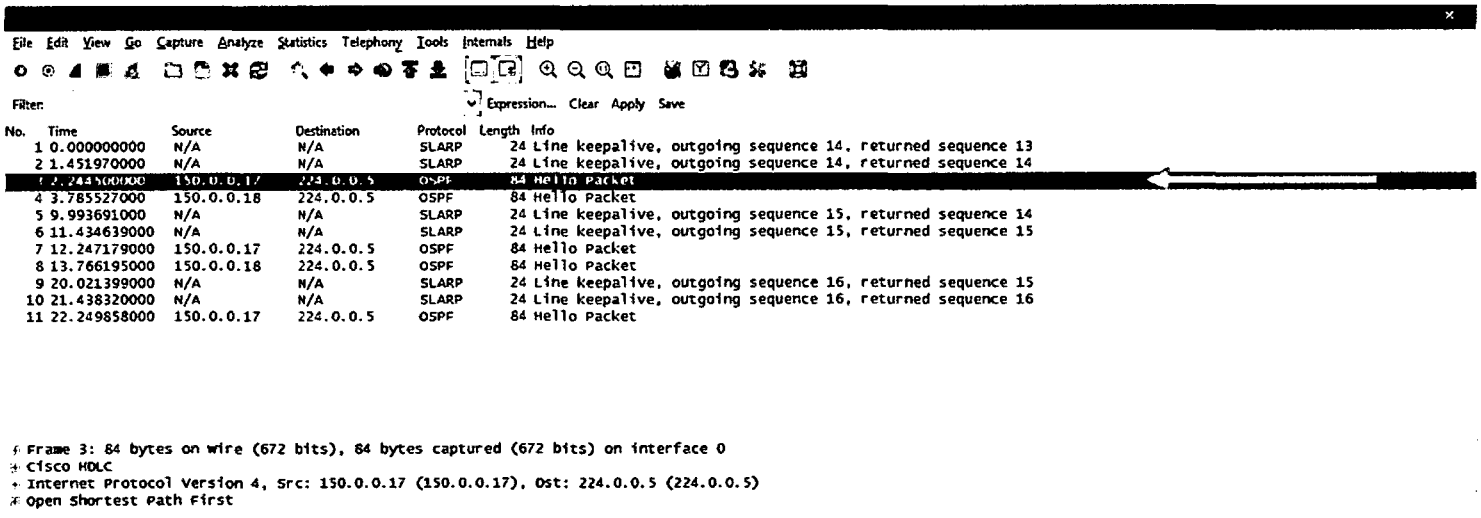
En la figura 4.5.20 se observa los valores del Jitter obtenidos al enviar diferentes tamaños de paquete UDP como 750, 1125 y 1500 bytes utilizando una velocidad de Tx constante de 0.5 Mbps, se puede observar claramente que con una trama de 750 bytes se tiene un Jitter de 0.433 ms a diferencia de la trama de 1500 bytes en la cual se tiene un Jitter de 1.036 ms.

En la figura 4.5.21, se observa los valores del Jitter obtenidos al enviar paquetes UDP de 1470 bytes utilizando una velocidad de Tx que varía de: 0.1 Mbps, 0.5 Mbps y 0.8 Mbps, sin que se pierdan paquetes en la red

PASO 4: Captura de tráfico con Wireshark.

Capturar tráfico de paquetes en la interfaz s0/2 de R3.

- Captura de paquetes HELLO OSPF.



- **Fig. 4.5.23 Captura de paquete HELLO OSPF con Wireshark.**

Información más detallada sobre el paquete HELLO.

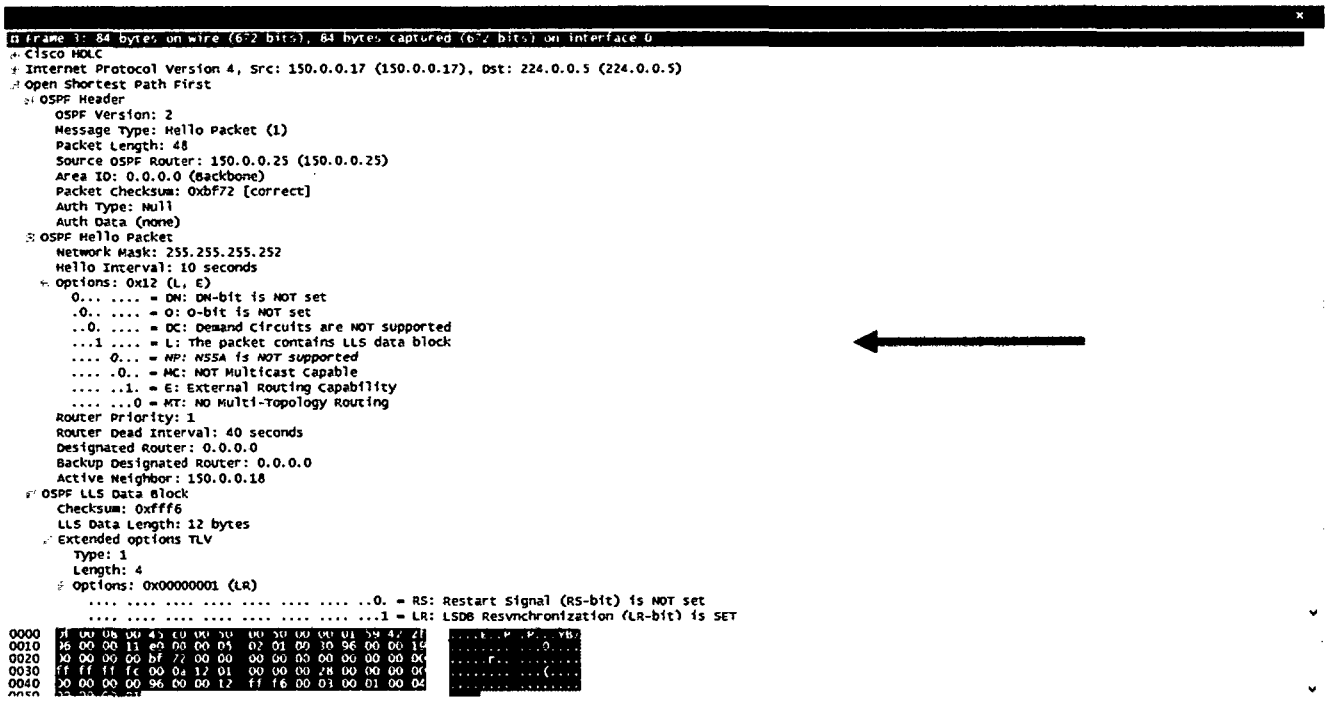


Fig. 4.5.24 Información detallada del paquete HELLO OSPF.

- Captura de paquetes CDP (Cisco Discovery Protocol), permite descubrir dispositivos Cisco que estén directamente conectados.

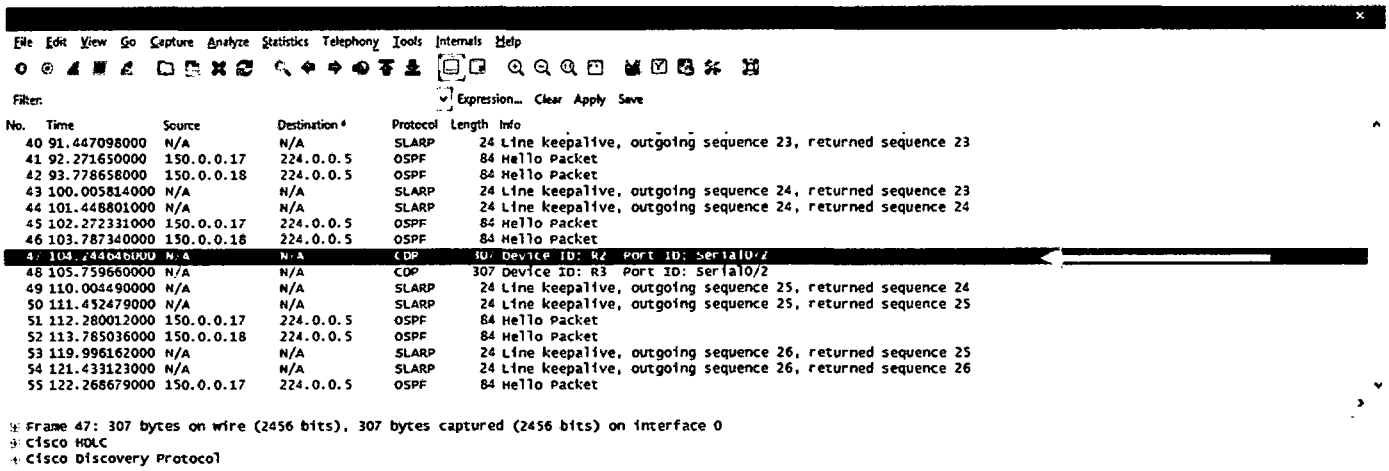


Fig. 4.5.25 Captura de paquete CDP con Wireshark.

Información más detallada sobre el dispositivo descubierto:

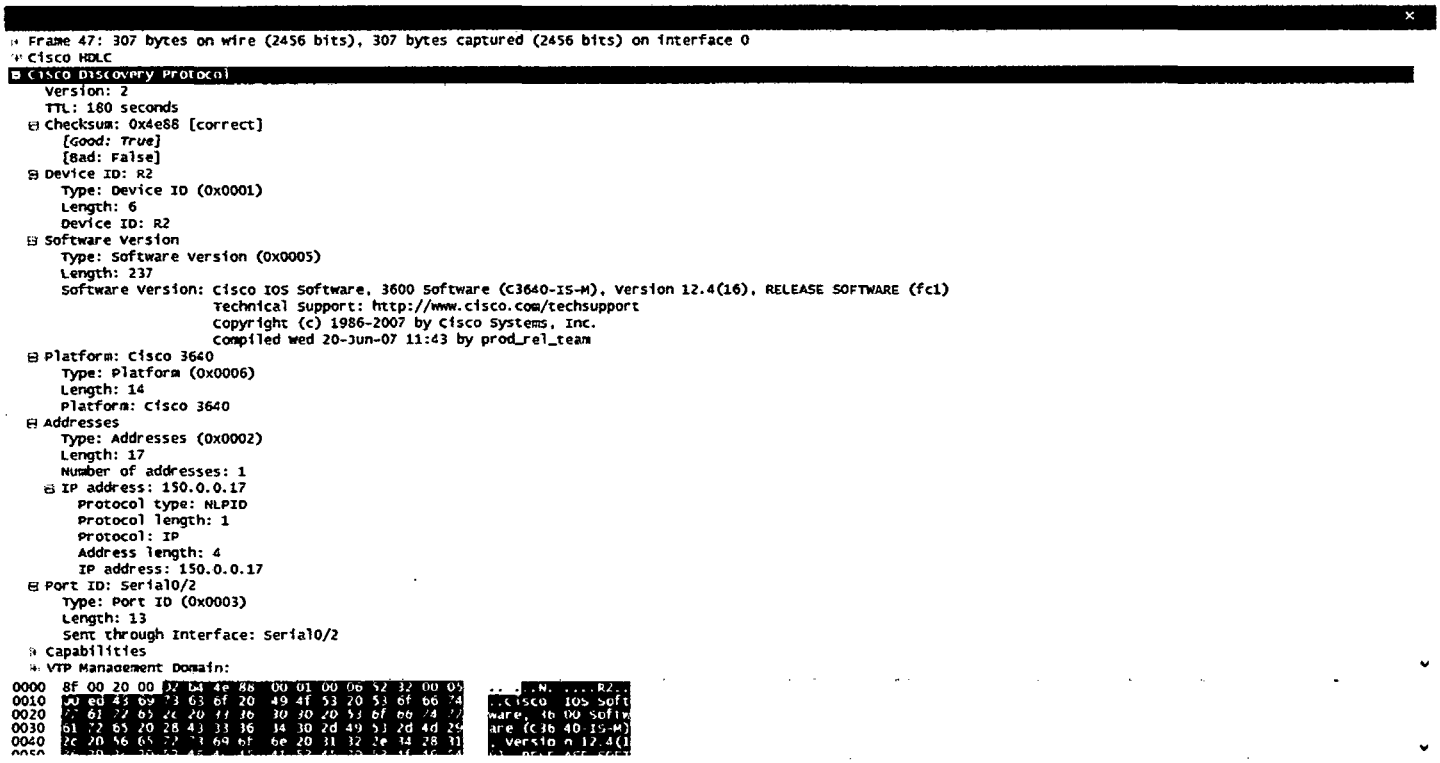


Fig. 4.5.26 Información detallada del paquete CDP.

Captura de paquetes ICMP.

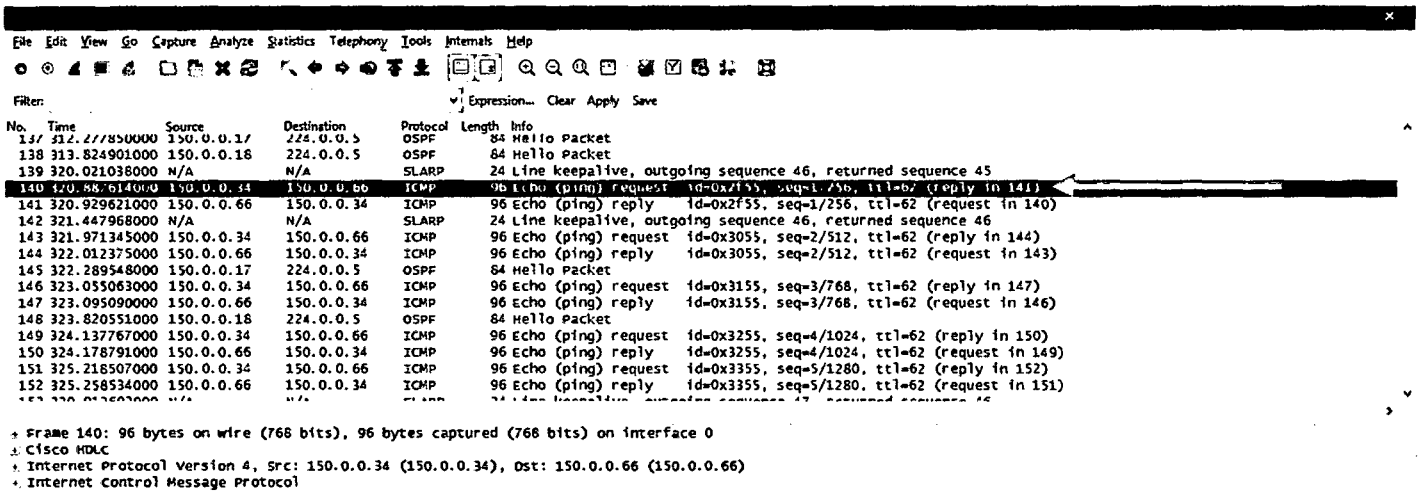


Fig. 4.5.27 Captura de paquetes ICMP con Wireshark.

Información más detallada sobre paquete ICMP:

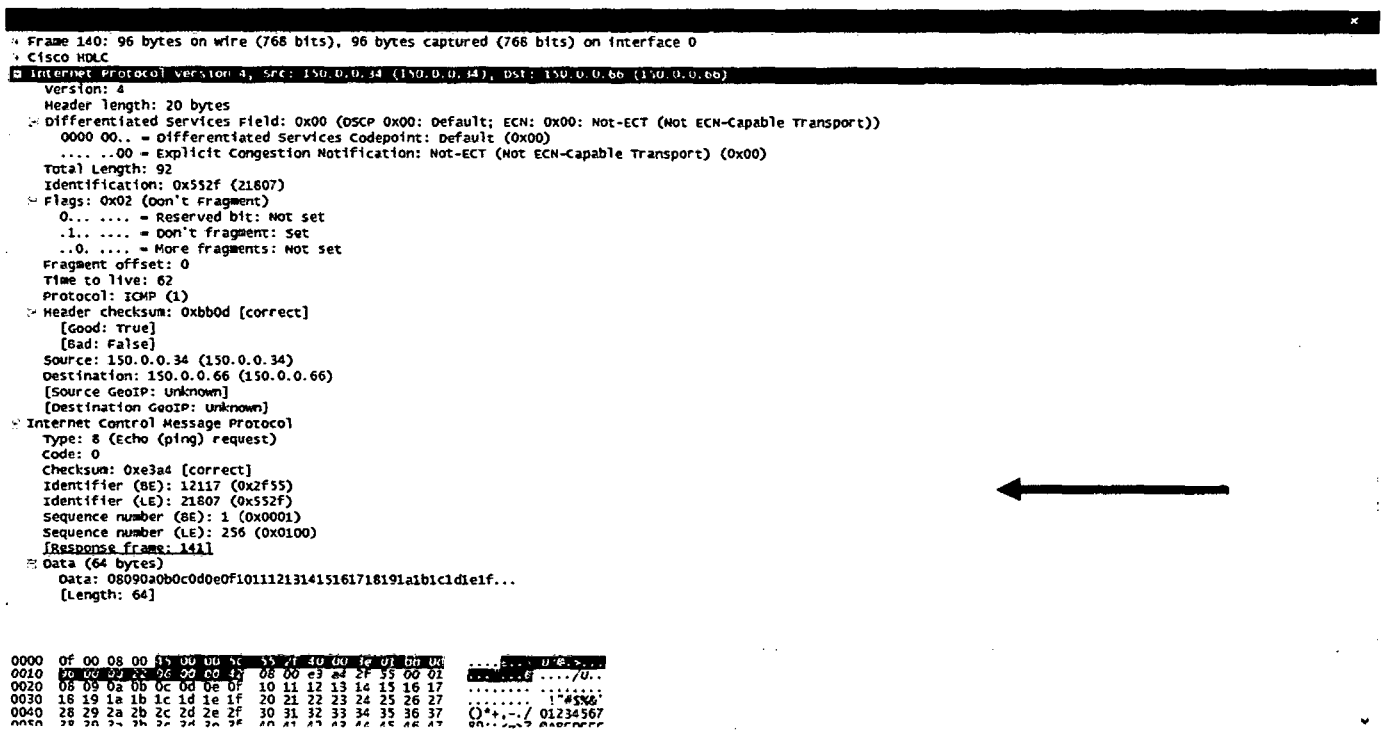


Fig. 4.5.28 Información detallada del paquete ICMP.

- Captura de paquetes Traceroute.

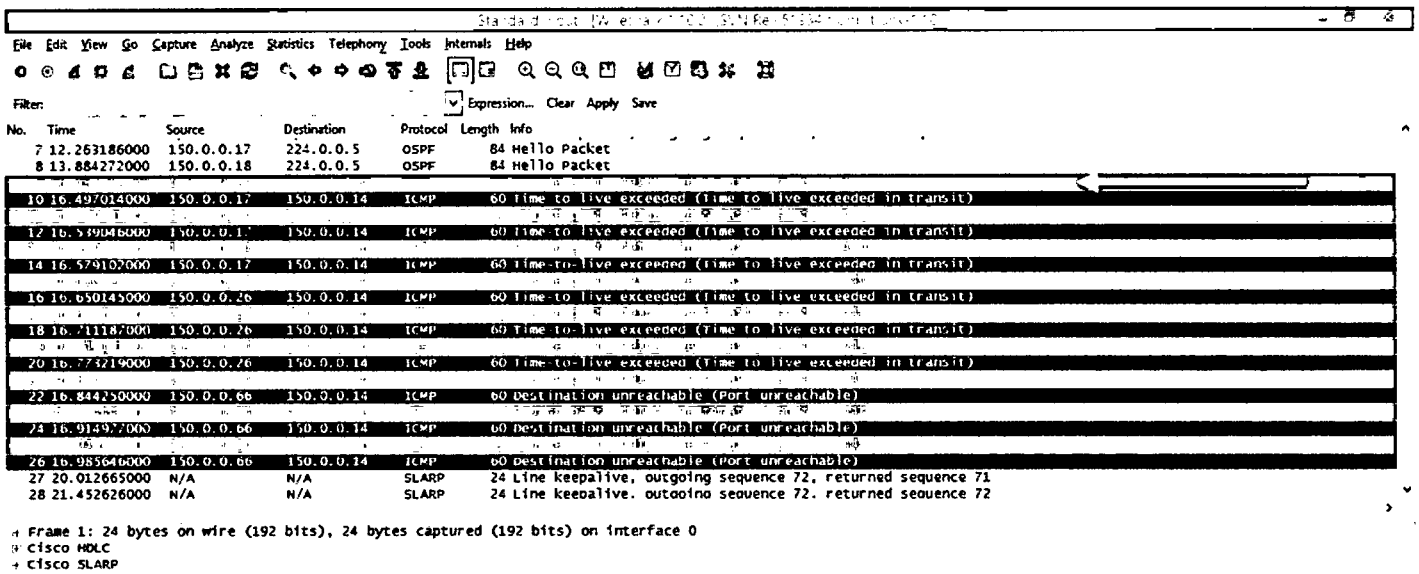


Fig. 4.5.29 Captura de paquetes Traceroute con Wireshark.

- Captura de paquetes Telnet

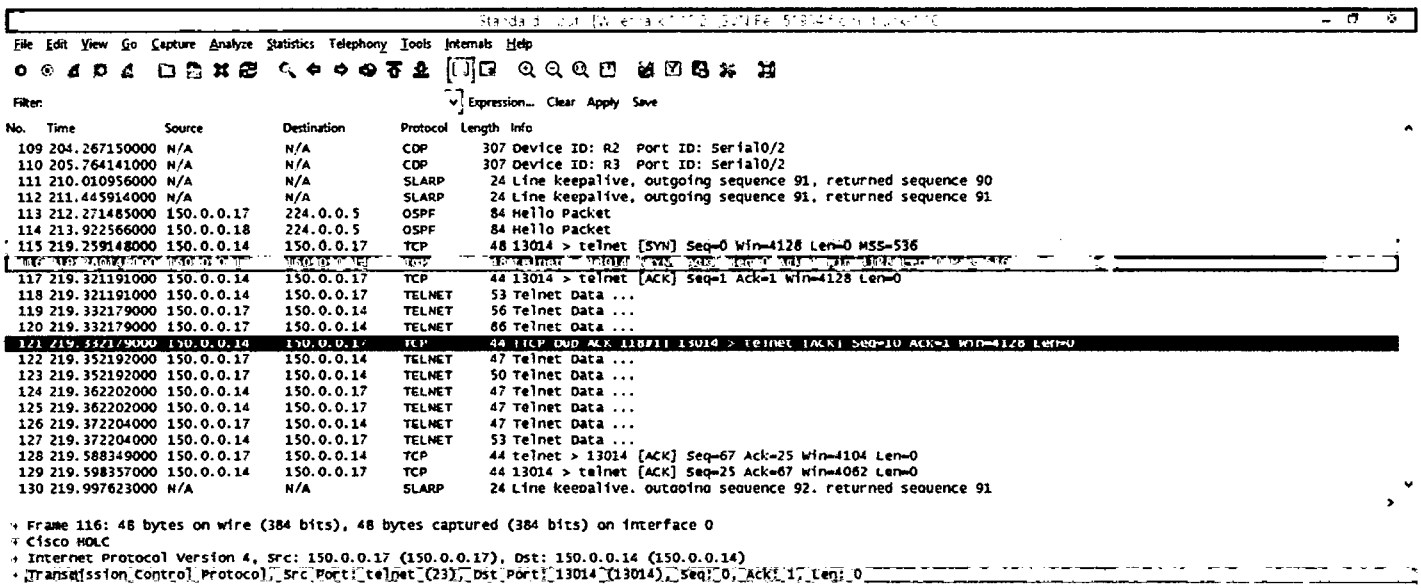


Fig. 4.5.30 Captura de paquete telnet con Wireshark.

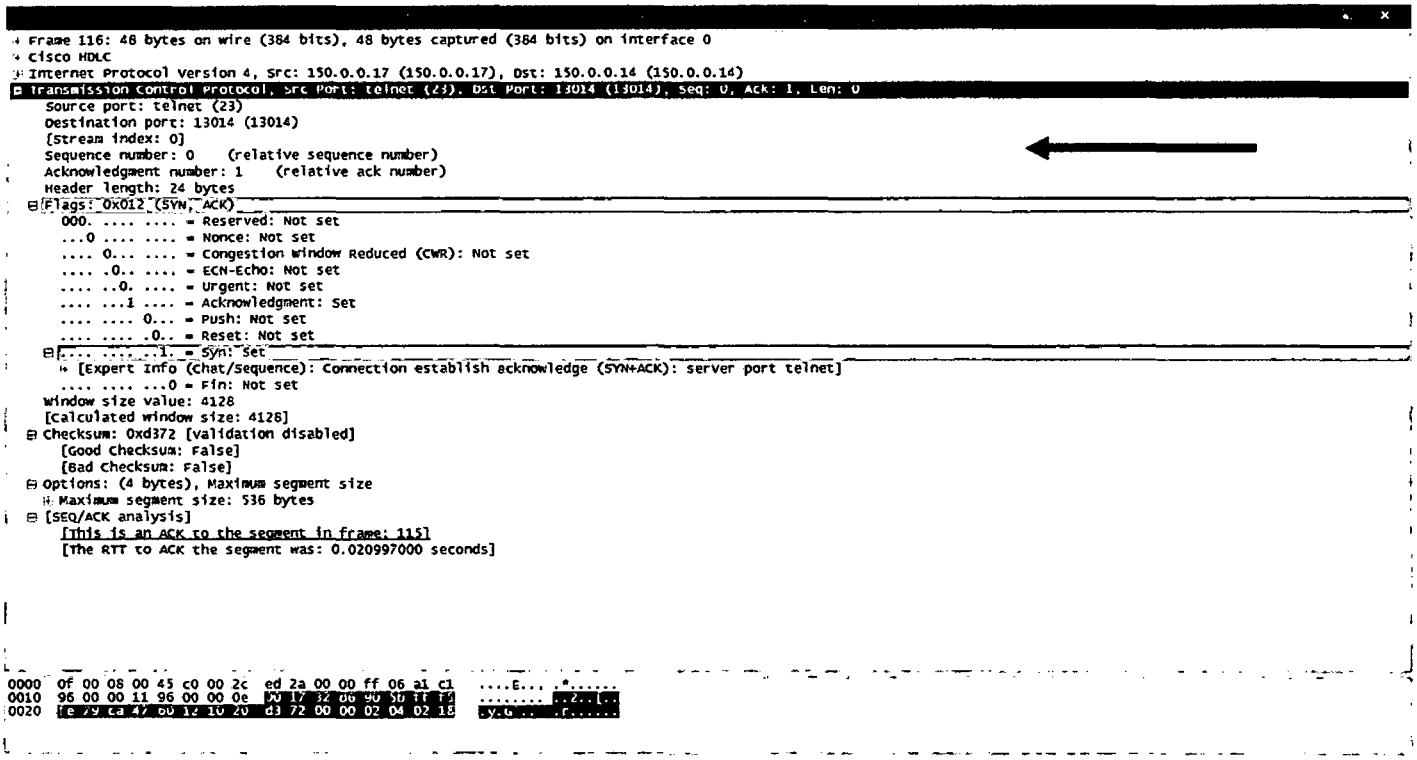


Fig. 4.5.31 Información detallada del paquete telnet.

LABORATORIO 4.6: CONFIGURACION BASICA DE BGP

REVISIÓN TEÓRICA: Para la realización de esta práctica se deberá revisar conceptos de BGP.

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar interfaces.
- Configurar el enrutamiento BGP externo (eBGP) en los routers de borde.
- Configurar el enrutamiento BGP interno (iBGP) en los routers del mismo AS.
- Configurar el enrutamiento OSPF en todos los routers conforme su AS.
- Configurar las ID del router OSPF.
- Verificar el enrutamiento OSPF por medio de los comandos show.
- Verificar el enrutamiento BGP por medio de los comandos show.

ESCENARIOS:

En esta actividad de laboratorio el usuario aprenderá a configurar el protocolo de enrutamiento eBGP en los routers de borde y de configurar iBGP junto a OSPF en los routers de mismo AS en la red que se muestra en el Diagrama de topología, eBGP es utilizado para definir la relación entre diferentes sistemas autónomos en una red de IP. El laboratorio estará dividido en dos redes diferentes una con un sistema autónomo (AS) 100 y la otra con AS 200, y los equipos que pertenecen a cada una de las redes trabajarán juntos como parte de la misma, tenga en cuenta los siguientes requisitos para el direccionamiento IP de las redes LAN:

LAN R2: 200 host.

LAN R5: 150 host.

Utilice las direcciones dadas en la tabla para la configuración de las interfaces LAN y WAN.

DIAGRAMA DE TOPOLOGÍA:

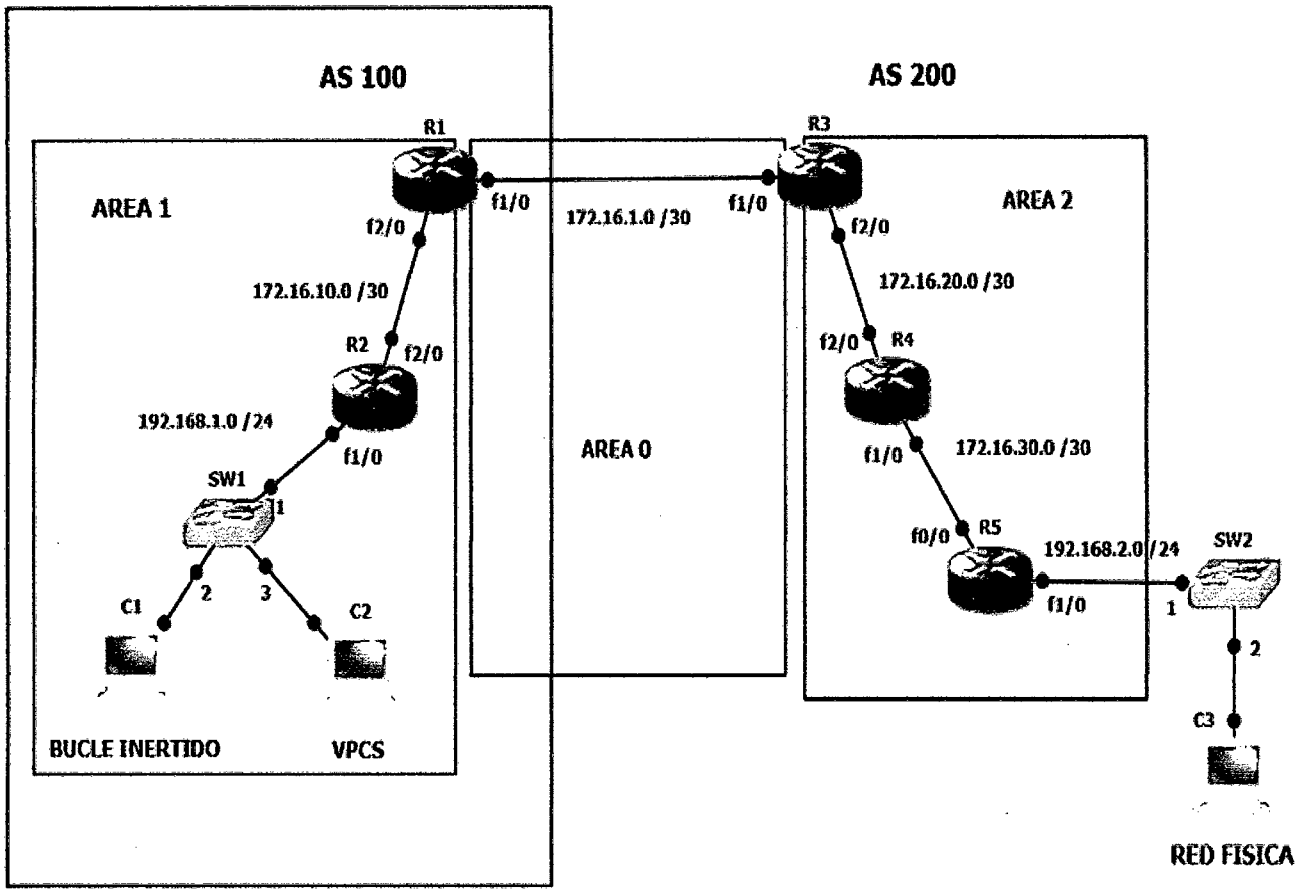


Fig. 4.6.1 Diagrama de topología en GNS3.

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN:

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	f1/	172.16.1.1	255.255.255.252	No aplicable
	f2/0	172.16.10.1	255.255.255.252	No aplicable
R2	f1/0	192.168.1.1	255.255.255.0	No aplicable
	f2/0	172.16.10.2	255.255.255.252	No aplicable
R3	f1/0	172.16.1.2	255.255.255.252	No aplicable
	f2/0	172.16.20.1	255.255.255.252	No aplicable
R4	f1/0	172.16.30.1	255.255.255.252	No aplicable
	f2/0	172.16.20.2	255.255.255.252	No aplicable
R5	g0/1	192.168.2.1	255.255.255.0	No aplicable
	g0/0	172.16.30.2	255.255.255.252	No aplicable
C1	VPCS	192.168.1.3	255.255.255.0	192.168.1.1
C2	BUCLE INVERTIDO	192.168.1.2	255.255.255.0	192.168.1.1
PC REAL	NIC	192.168.2.2	255.255.255.0	192.168.2.1

Tabla 4.6.1 Direccionamiento IP para las Redes

TAREA 1: MONTAR LA RED EN GNS3

Montar y conectar la red igual a la del Diagrama de topología.

TAREA 2: REALIZAR LA CONFIGURACIÓN BÁSICA DEL ROUTER

Configure los routers R1, R2, R3, R4, y R5 de acuerdo a las siguientes instrucciones desde el modo de configuración:

PASO 1: Configure el nombre de host del router.

PASO 2: Deshabilite la búsqueda DNS.

PASO 3: Configure una contraseña de Modo EXEC.

PASO 4: Configure un mensaje del día.

PASO 5: Configure una contraseña para las conexiones de la consola.

PASO 6: Configure una contraseña para las conexiones de vty.

PASO 7: Configure el registro de datos sincrónico.

PASO 8: Guardar la configuración en cada router.

TAREA 3: CONFIGURAR Y ACTIVAR LAS DIRECCIONES FASTETHERNET

PASO 1: Configurar las interfaces de los routers.

Configure las interfaces de los routers R1, R2, R3, R4, R5 con las direcciones IP de la tabla de direccionamiento que se encuentra al comienzo de esta práctica de laboratorio.

R1:

Configuración para una interface fasEthernet:

R1(config)# **interface fasEthernet 1/0**

R1(config-if)# **description conexion a R3**

R1(config-if)# **ip address 172.16.1.1 255.255.255.252**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface fasEthernet 2/0**

R1(config-if)# **description conexion a R2**

R1(config-if)# **ip address 172.16.10.1 255.255.255.252**

R1(*config-if*)# **no shutdown**

R1(config-if)# **exit**

Nota: Seguir los mismos pasos para la configuacion de las interfaces de los demás routers.

PASO 2: Configurar las interfaces Loopback en todos los routers según corresponda.

R1: 1.1.1.1 /32

R2: 2.2.2.2 /32

R3: 3.3.3.3 /32

R4: 4.4.4.4 /32

R5: 5.5.5.5 /32

R1(config)#**interface loopback 1**

R1(config)# **ip address 1.1.1.1 255.255.255.255**

R1(config)# **exit**

PASO 3: Guardar la configuración.

TAREA 4: CONFIGURAR OSPF EN LOS ROUTERS

Configure el protocolo de enrutamiento OSPF en todos los routers de la red para la conectividad.

Los enrutadores dentro de la red, estarán distribuidos en 3 áreas diferentes área 0, área 1 y área 2 de OSPF, asegúrese de configurarlos de acuerdo a la red donde se encuentren conforme indica en el diagrama de topologia.

R1(config)# **router ospf 100**

R1(config-router)# **network 172.16.1.0 0.0.0.3 area 0**

R1(config-router)# **network 1.1.1.1 0.0.0.0 area 1**

R1(config-router)# **network 172.16.10.0 0.0.0.3 area 1**

R1(config-router)# **passive-interface fastethernet 1/0**

R1(config-router)# **exit**

R2(config)#**router ospf 100**

R2(config-router)#**network 172.16.10.0 0.0.0.3 area 1**

R2(config-router)#**network 2.2.2.2 0.0.0.0 area 1**

R2(config-router)#**network 192.168.1.0 0.0.0.255 area 1**

R2(config-router)# **passive-interface fastethernet 1/0**

R2(config-router)#**exit**

NOTA: Configurar el protocolo OSPF en los demás routers de la misma forma.

TAREA 5: CONFIGURAR EL PROTOCOLO BGP EN LOS ROUTERS

PASO 1: Configuracion de eBGP en los routers de borde:

R1(config)# **router bgp 100**

R1(config-router)# **neighbor 172.16.1.2 remote-as 200**

R1(config-router)# **neighbor 2.2.2.2 remote-as 100**

R1(config-router)# **neighbor 2.2.2.2 update-source loopback 1**

R1(config-router)# **network 1.1.1.1 mask 255.255.255.255**

R1(config-router)# **network 2.2.2.2 mask 255.255.255.255**

R1(config-router)# **network 192.168.1.0 mask 255.255.255.0**

R1(config-router)# **no synchronization**

R1(config-router)# no **auto-summary**

R1(config-router)# **exit**

R3(config)# **router bgp 200**

R3(config-router)# **neighbor 172.16.1.1 remote-as 100**

R3(config-router)# **neighbor 4.4.4.4 remote-as 200**

R3(config-router)# **neighbor 4.4.4.4 update-source loopback 1**

R3(config-router)# **neighbor 4.4.4.4 route-reflector-client**

R3(config-router)# **neighbor 5.5.5.5 remote-as 200**

R3(config-router)# **neighbor 5.5.5.5 update-source loopback 1**

R3(config-router)# **neighbor 5.5.5.5 route-reflector-client**

R3(config-router)# **network 3.3.3.3 mask 255.255.255.255**

R3(config-router)# **network 4.4.4.4 mask 255.255.255.255**

R3(config-router)# **network 5.5.5.5 mask 255.255.255.255**

R3(config-router)# **network 192.168.1.0 mask 255.255.255.0**

R3(config-router)# **no synchronization**

R3(config-router)#**no auto-summary**

R3(config-router)# **exit**

PASO 2: Configuracion de iBGP en los enrutadores del mismo AS:

Use la dirección de la interfase de loopback para las sesiones de iBGP.
R4(config)# **router bgp 200**

R4(config-router)# **no synchronization**

R4(config-router)# **neighbor 3.3.3.3 remote-as 200**

R4(config-router)# **neighbor 3.3.3.3 update-source loopback 1**

R4(config-router)# **neighbor 5.5.5.5 remote-as 200**

R4(config-router)# **neighbor 5.5.5.5 update-source loopback 1**

R4(config-router)#**no auto-summary**

R4(config-router)# **exit**

NOTA: Seguir los mismos pasos de configuración de iBGP para los routers faltantes.

PASO 3: Redistribución de direcciones IP en diferentes sistemas autónomos:

Los router de borde intercambian en las actualizaciones BGP las direcciones IP que reciben, dichas direcciones se envían desde el router R1 a R3 o viceversa.

R3(config-router) # **router bgp 200**

R3(config-router)# **redistribute ospf 200**

R3(config-router)# **bgp redistribute-internal**

R3(config-router)# **exit**

R3(config-router)# **router ospf 200**

R3(config-router)# **redistribute bgp 200 subnets**

R3(config-router)# **exit**

R1(config-router) # **router bgp 100**

R1(config-router)# **redistribute ospf 100**

R1(config-router)# **bgp redistribute-internal**

R(config-router)# **exit**

R1(config-router)# **router ospf 100**

R1(config-router)# **redistribute bgp 100 subnets**

R1(config-router)# **exit**

TAREA 6: CONFIGURAR LOS EQUIPOS DE HOST.

Configurar las direcciones IP y gateways por defecto como se indican en la tabla de direccionamiento de las interfaces Ethernet de C1, C2 (VPCS) y PC REAL.

TAREA 7: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

PASO 1: Verificar el direccionamiento IP y las interfaces.

R1#**show ip interface brief**

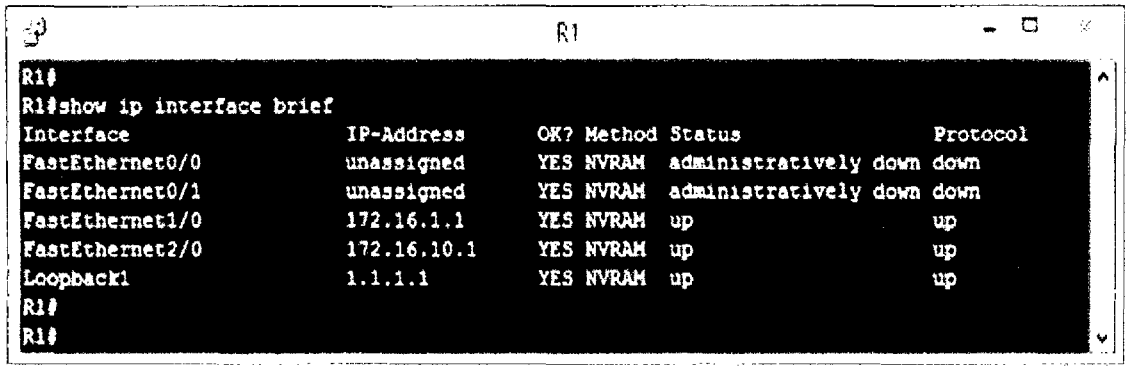


Fig. 4.6.2 Tabla ip de interface brief de R1.

NOTA: Verificar que las interfaces de los demás routers tengan la adecuada dirección IP y estén activas.

PASO 2: Verificar la configuración de los router. Use los comandos **show ip route** para verificar el contenido de la tabla de enrutamiento.

R2#**show ip route**

```
R1#
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback1
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/2] via 172.16.10.2, 02:06:05, FastEthernet2/0
     3.0.0.0/32 is subnetted, 1 subnets
B       3.3.3.3 [20/0] via 172.16.1.2, 00:15:21
     4.0.0.0/32 is subnetted, 1 subnets
B       4.4.4.4 [20/2] via 172.16.1.2, 00:14:51
     5.0.0.0/32 is subnetted, 1 subnets
B       5.5.5.5 [20/3] via 172.16.1.2, 00:14:51
     172.16.0.0/30 is subnetted, 4 subnets
B       172.16.30.0 [20/2] via 172.16.1.2, 00:14:53
B       172.16.20.0 [20/0] via 172.16.1.2, 00:15:23
C       172.16.10.0 is directly connected, FastEthernet2/0
C       172.16.1.0 is directly connected, FastEthernet1/0
O    192.168.1.0/24 [110/2] via 172.16.10.2, 02:06:09, FastEthernet2/0
B    192.168.2.0/24 [20/3] via 172.16.1.2, 00:14:56
R1#
```

Fig. 4.6.3 Tabla de enrutamiento de R1.

```
R3#
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
B       1.1.1.1 [20/0] via 172.16.1.1, 00:34:59
     2.0.0.0/32 is subnetted, 1 subnets
B       2.2.2.2 [20/2] via 172.16.1.1, 00:34:59
     3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3 is directly connected, Loopback1
     4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/2] via 172.16.20.2, 00:34:46, FastEthernet2/0
     5.0.0.0/32 is subnetted, 1 subnets
O       5.5.5.5 [110/3] via 172.16.20.2, 00:34:46, FastEthernet2/0
     172.16.0.0/30 is subnetted, 4 subnets
O       172.16.30.0 [110/2] via 172.16.20.2, 00:34:48, FastEthernet2/0
C       172.16.20.0 is directly connected, FastEthernet2/0
B       172.16.10.0 [20/0] via 172.16.1.1, 00:35:01
C       172.16.1.0 is directly connected, FastEthernet1/0
B    192.168.1.0/24 [20/2] via 172.16.1.1, 00:35:01
O    192.168.2.0/24 [110/3] via 172.16.20.2, 00:34:48, FastEthernet2/0
R3#
```

Fig. 4.6.4 Tabla de enrutamiento de R3.

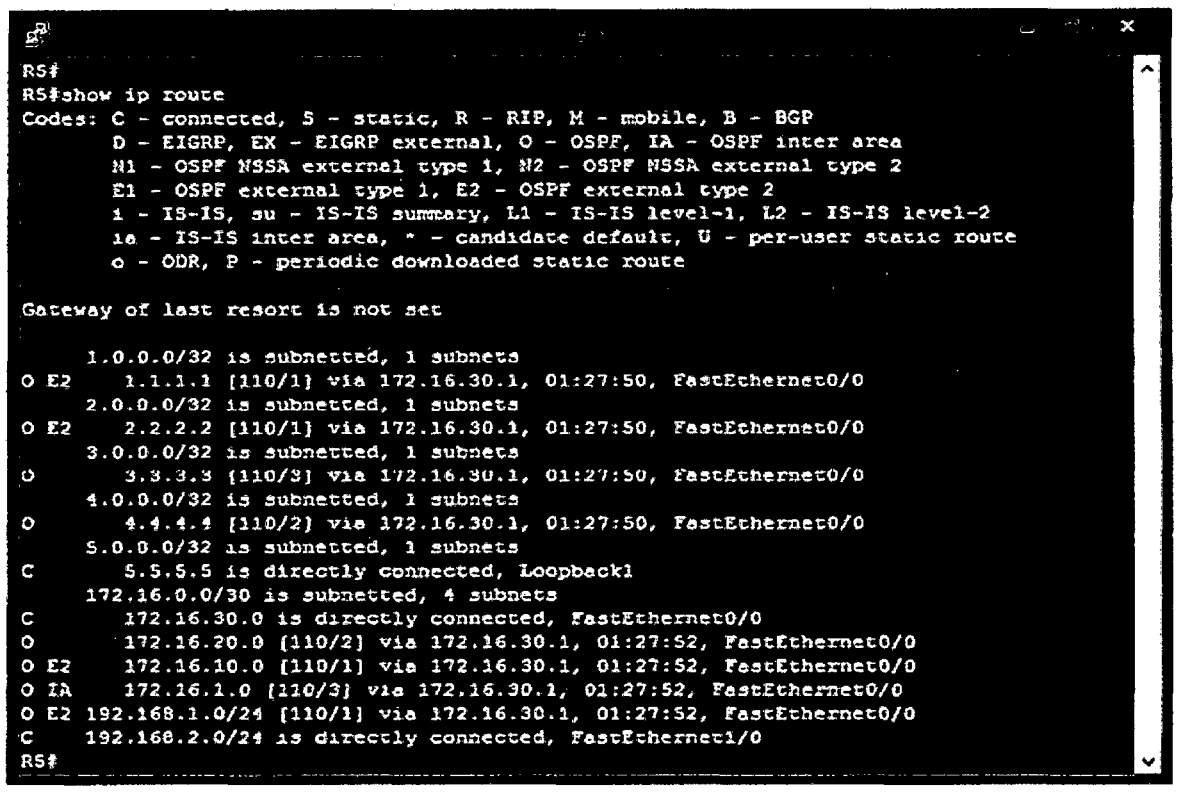


Fig. 4.6.5 Tabla de enrutamiento de R5.

NOTA: Verificar de igual manera la tabla de enrutamiento de los demás routers.

PASO 3: Verificamos la configuración de BGP en los routers, con el comando **show ip bgp**, como se muestra a continuación.

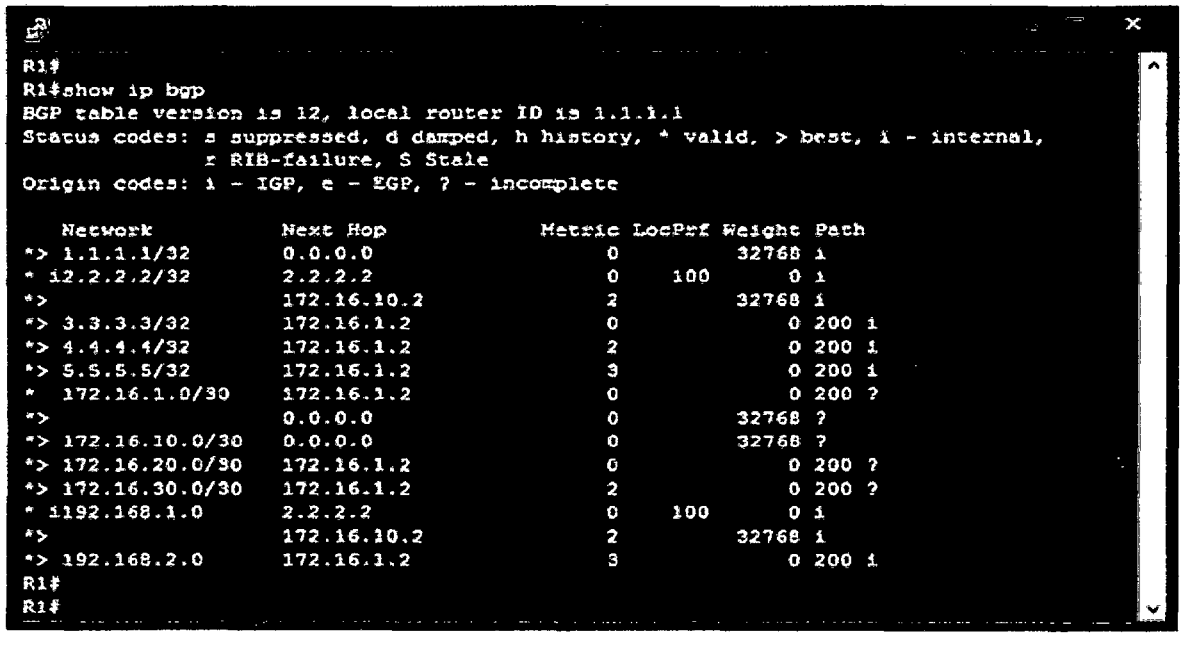


Fig. 4.6.6 Tabla de Configuración de BGP en R1.

R3#**show ip bgp**

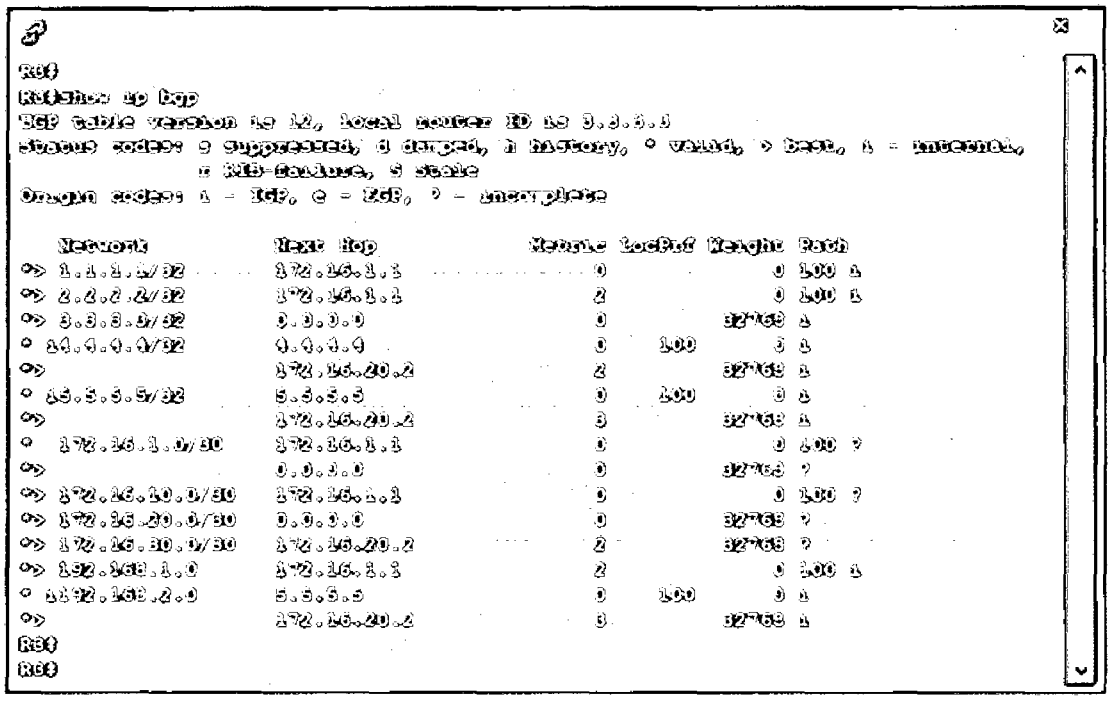


Fig. 4.6.7 Tabla de Configuración de BGP en R3.

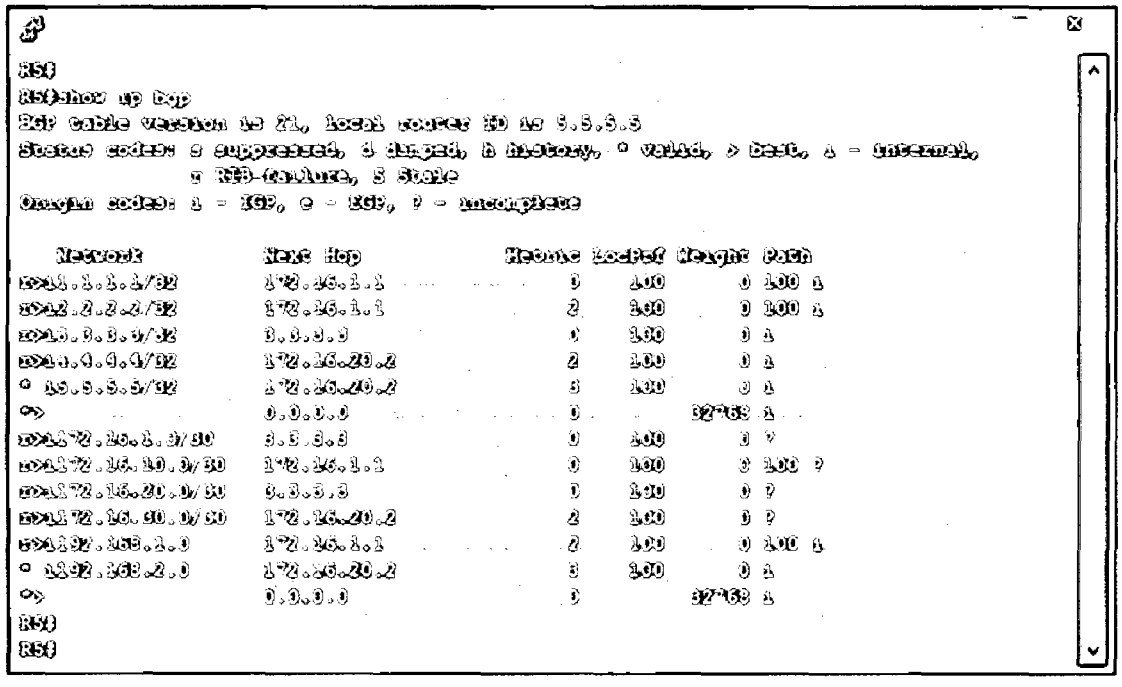


Fig. 4.6.8 Tabla de Configuración de BGP en R5.

NOTA: Verificar de la misma manera la tabla de configuración de BGP en los routers faltantes.

PASO 4: Utilice le comando **show ip bgp summmary** para verificar la adecuada configuración del protocolo BGP en la red.

R1#show ip bgp summary

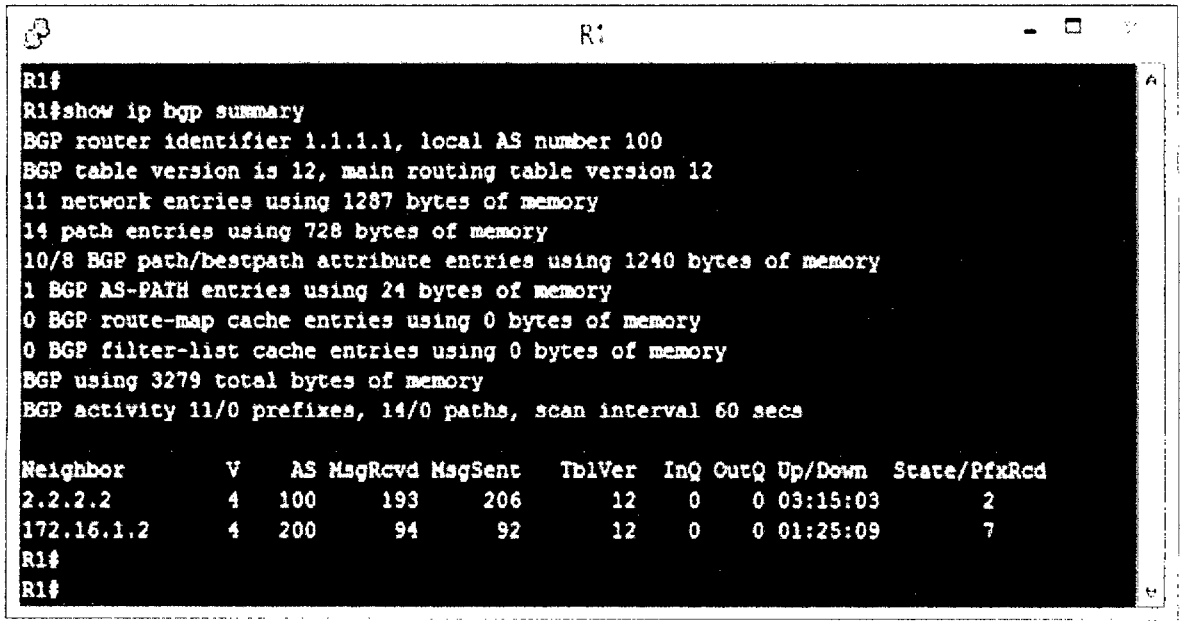


Fig. 4.6.9 Verificación de la configuración de BGP.

NOTA: Verificar en los demás routers la correcta configuración de iBGP y eBGP de la misma manera.

PASO 5: Verificar que hay conectividad completa en la red.

Use el comando **ping** para verificar la conectividad.

R5#**ping 192.168.1.1**

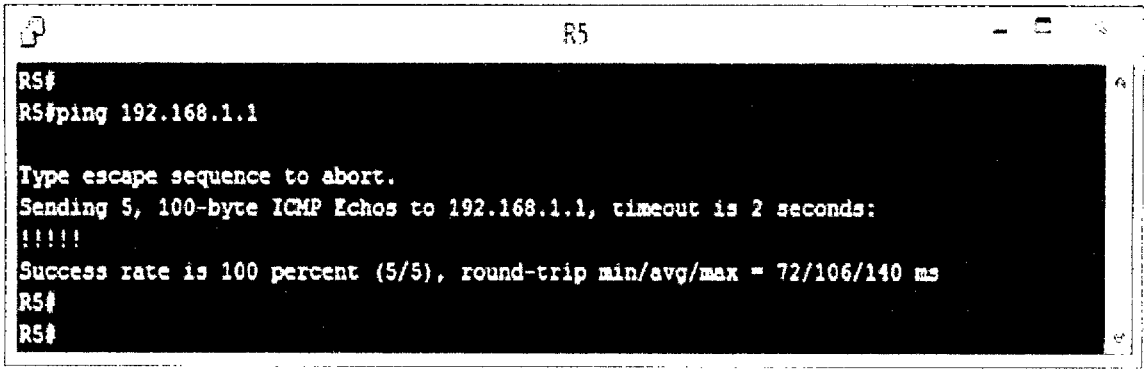


Fig. 4.6.10 Prueba de conectividad entre R5 y R2.

R2#ping 192.168.2.1

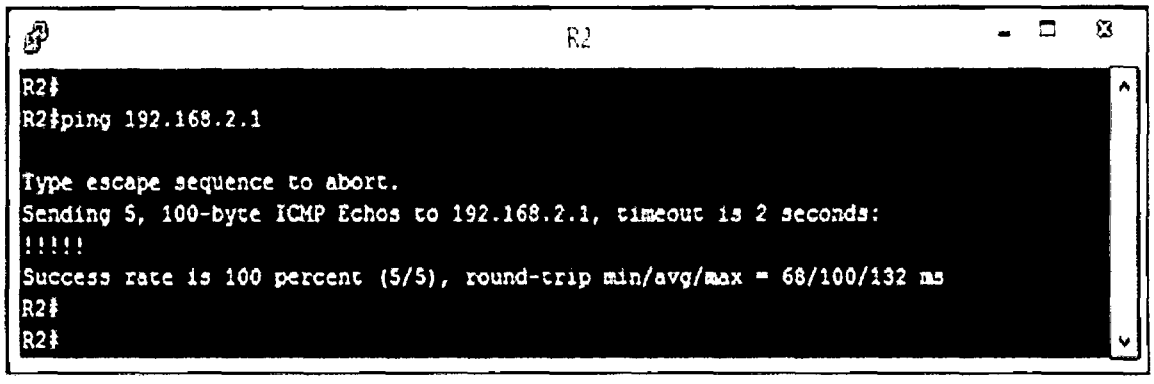


Fig. 4.6.11 Prueba de conectividad entre R2 y R5.

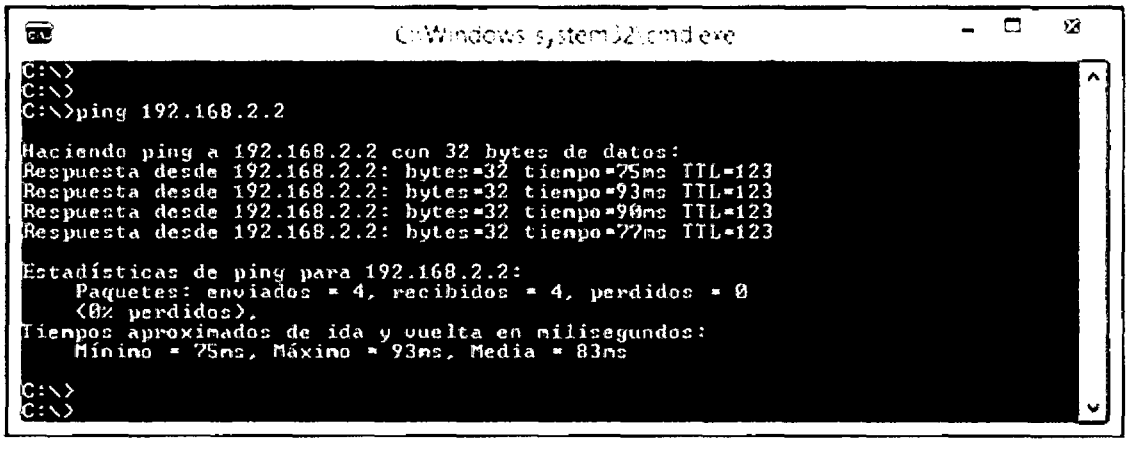


Fig. 4.6.12 Prueba de conectividad entre host desde C1 a PC real.

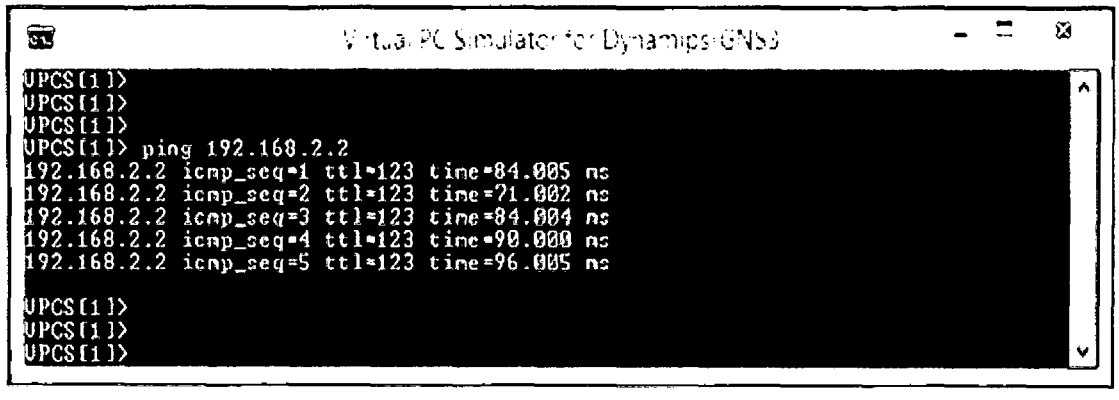


Fig. 4.6.13 Prueba de conectividad entre host desde C2 a PC real.

TAREA 8: ANALISIS DEL TRAFICO DE PAQUETES

PASO 1: Medición de la Latencia

Para la medición de la latencia se realizó 10 muestras sucesivas de 100 ping desde el C1 (Bucle invertido) hacia la PC REAL considerando un tamaño de trama de 64, 512 y 1518 bytes como se especifica en el RFC 2544.

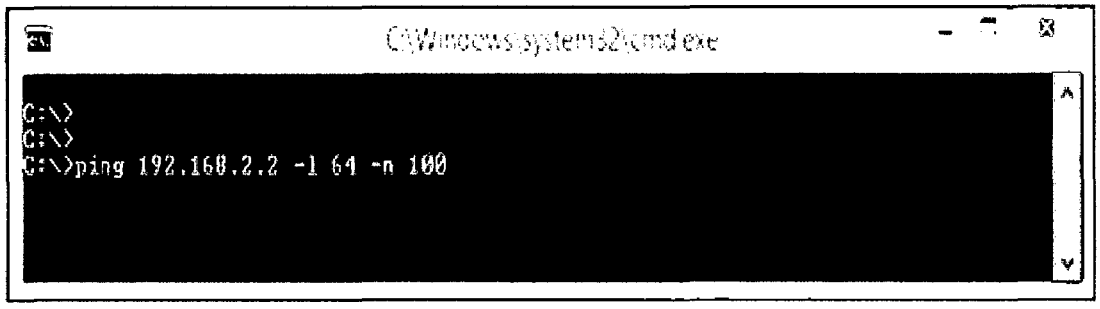


Fig. 4.6.14 Forma de medición de la latencia.

En la Figura 4.10.15 se puede observar el envío de 100 ping con una trama de 64 hacia la dirección 192.168.2.2

En las Tablas posteriores se detallan los valores de la Latencia que se ha obtenido una vez realizadas todas las muestras.

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	N° 1	**N° 2**	**N° 3**	**N° 4**	**N° 5**	**N° 6**	**N° 7**	**N° 8**	**N° 9**	**N° 10**	**Promedio**
Tiempo Mínimo (ms)	**70**	**71**	**70**	**71**	**68**	**70**	**60**	**59**	**67**	**66**	**67.2**
Tiempo Máximo (ms)	**277**	**375**	**279**	**185**	**245**	**264**	**325**	**324**	**184**	**241**	**269.9**
Tiempo Promedio (ms)	**123**	**135**	**131**	**102**	**115**	**118**	**119**	**119**	**114**	**131**	**120.7**

Tabla 4.6.2 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	512										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	66	74	60	67	67	75	71	75	71	68	69.4
Tiempo Máximo (ms)	279	565	195	222	215	209	248	229	207	395	276.4
Tiempo Promedio (ms)	134	173	109	116	117	114	122	119	113	123	124.3

Tabla 4.6.3 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1518										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	71	79	65	68	72	76	73	70	76	72	72.2
Tiempo Máximo (ms)	178	599	183	286	272	293	359	236	363	237	300.6
Tiempo Promedio (ms)	125	163	114	124	125	137	129	128	150	141	133.6

Tabla 4.6.4 Comparación de datos obtenidos de las diferentes tramas.

LATENCIA			
Tamaño de Trama (bytes)	64	512	1518
Tiempo Mínimo (ms)	67.2	69.4	72.2
Tiempo Máximo (ms)	269.9	276.4	300.6
Tiempo Promedio (ms)	120.7	124.3	133.6

Tabla 4.6.5 Comparación de datos obtenidos de las diferentes tramas.

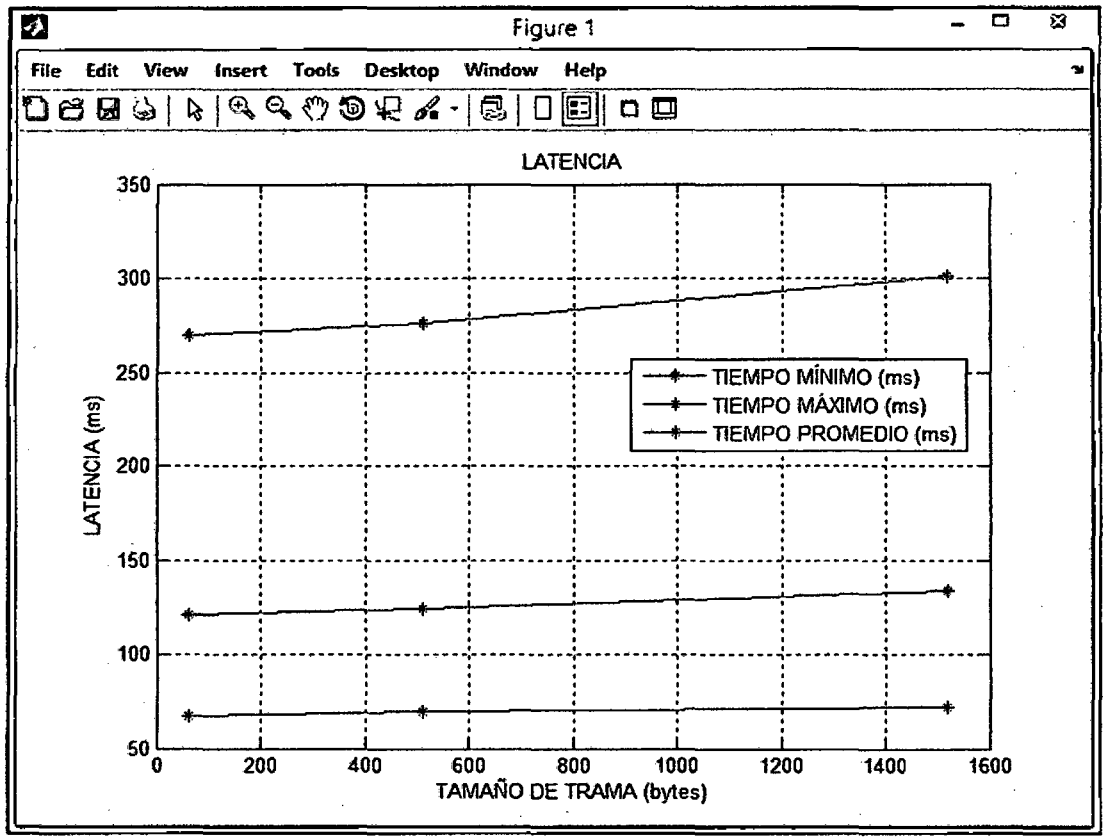


Fig. 4.6.15 Datos representados gráficamente de la variación de la latencia.

De acuerdo con los datos obtenidos, se puede observar claramente que los valores mínimo (color azul), máximo (color rojo) y promedio (color verde) de la latencia de la red se incrementan conforme se envía una trama de longitud mayor, en este caso con la trama de 1518 bytes se obtiene una latencia promedio de 148.8 ms a diferencia de una trama de 64 bytes con 118.5 ms.

PASO 2: Medición del Throughput

Para la medición del Throughput y Jitter se envió una cantidad de tramas a velocidades diferentes durante 20 segundos, hasta encontrar la máxima cantidad de tramas recibidas sin que se produzcan perdidas de las mismas en el router y PC REAL. Como se utilizó Jperf el cliente será el encargado de enviar los paquetes y el servidor los recibirá, indicando la cantidad de paquetes que llegaron correctamente considerando un tamaño del paquete UDP de 750, 1125, 1500 y 1470 (default) bytes, tal como se especifica en el RFC 768.

Configuración del Jperf como servidor para medir Throughput:

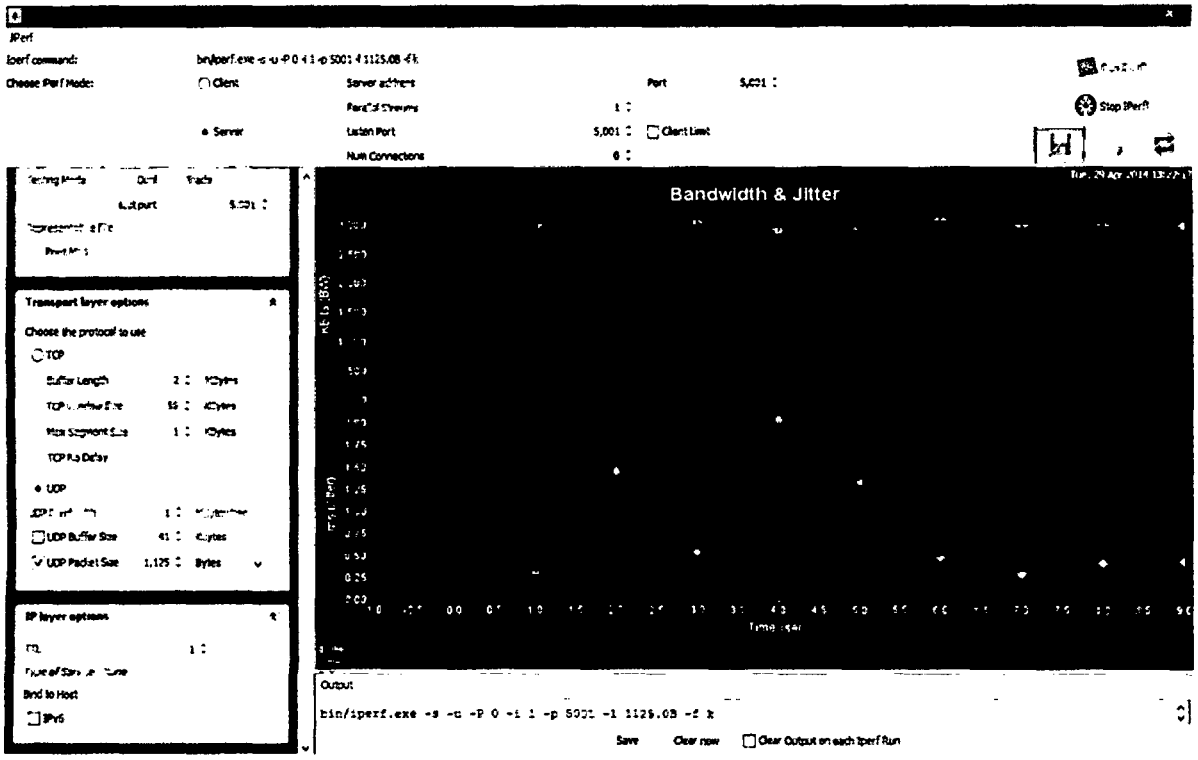


Fig. 4.6.16 Resultados al medir Throughput como servidor.

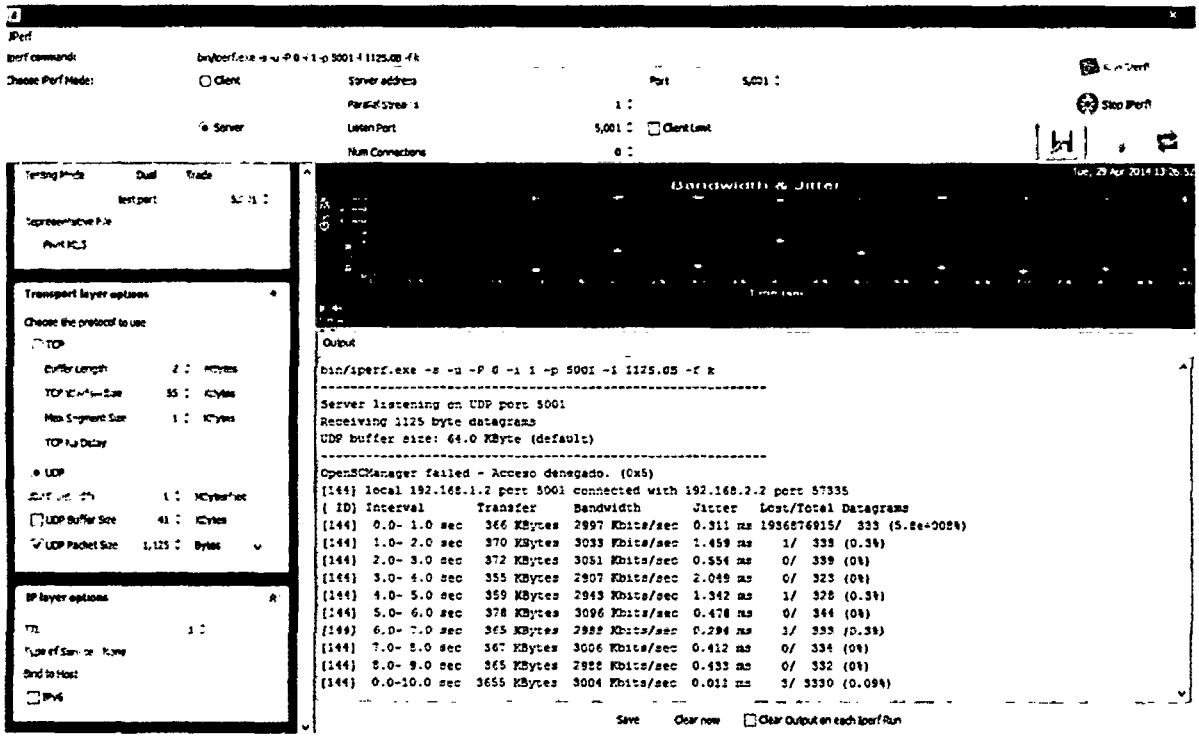


Fig. 4.6.17 Gráfica de Bandwidth y Jitter.

Configuración del Jperf como cliente para medir Throughput:

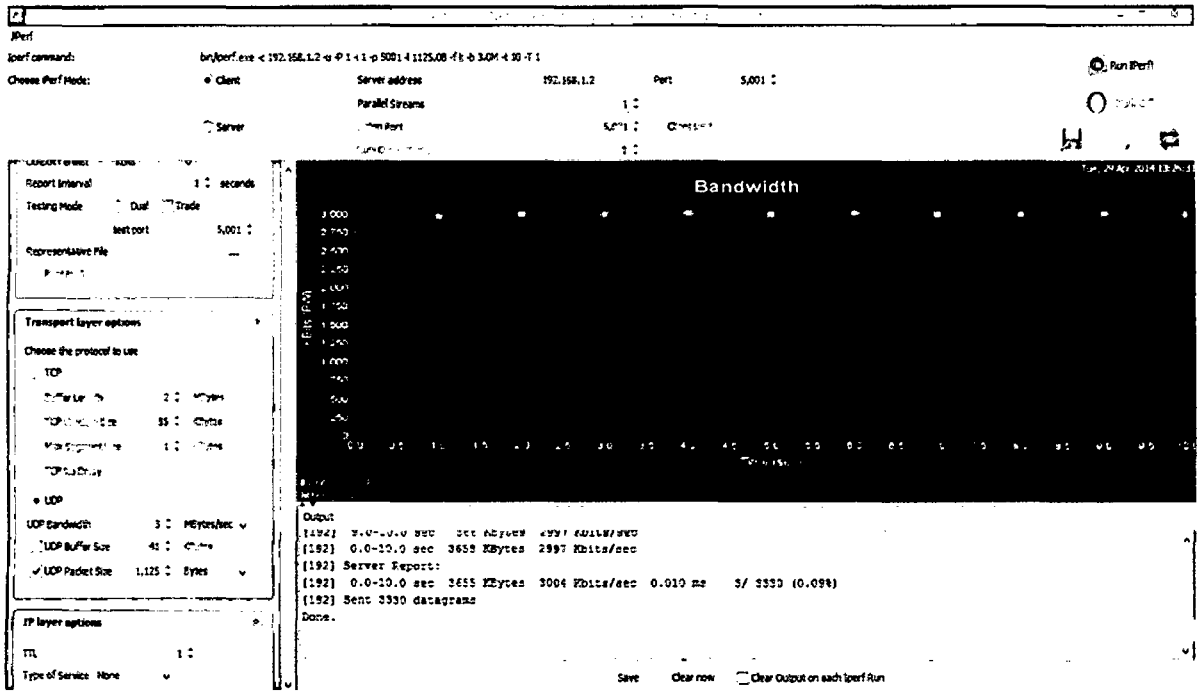


Fig. 4.6.18 Gráfica de Bandwidth.

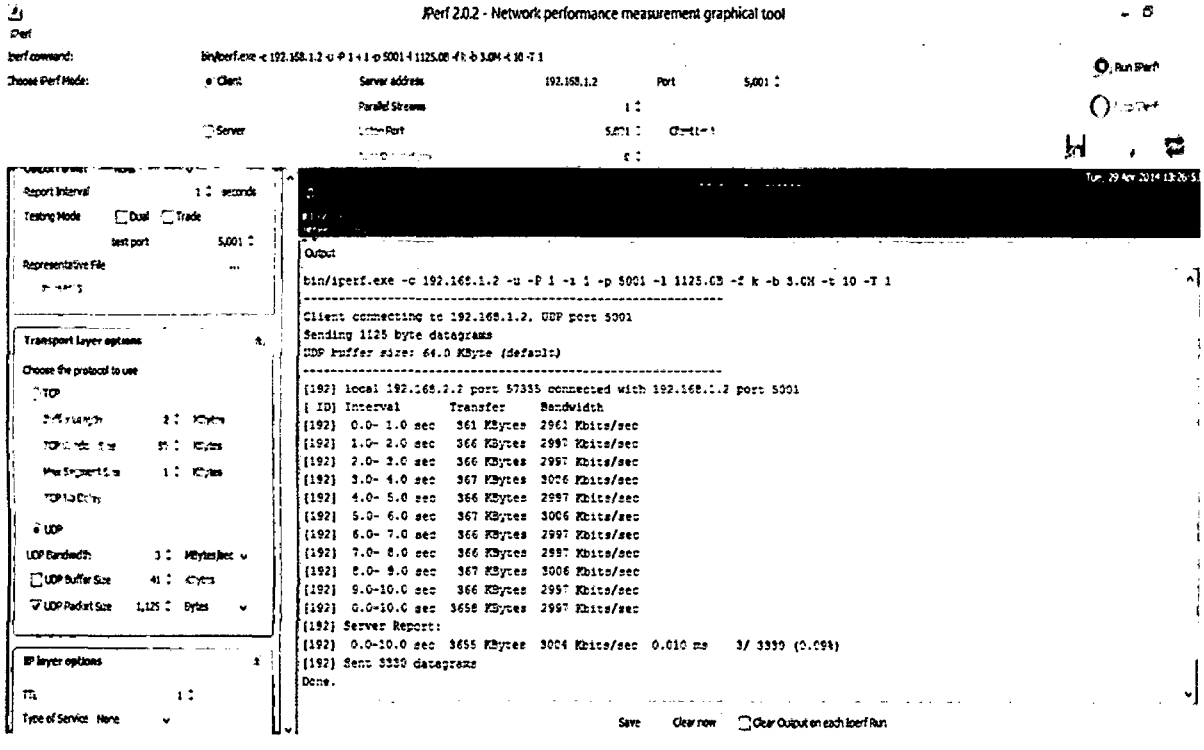


Fig. 4.6.19 Resultados del Jperf como Cliente al medir Throughput.

En las siguientes Tablas se detalla los valores del Throughput obtenidos una vez realizada todas las muestras.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**3**	**3**	**3**
Velocidad de Rx (Mbps)	**3**	**3**	**2.99**
Tramas Transmitidas	**4994**	**3330**	**2498**
Tramas Recibidas	**4994**	**3330**	**2498**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**500**	**333**	**250**

Tabla 4.6.6 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**1**	**5**	**7**	**10**
Velocidad de Rx (Mbps)	**1**	**4.97**	**6.83**	**7.24**
Tramas Transmitidas	**851**	**4247**	**5946**	**8505**
Tramas Recibidas	**851**	**4247**	**5946**	**8293**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**	**212 (2.5%)**
Tramas Recibidas (pps)	**85**	**425**	**594**	**850**

Tabla 4.6.7 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

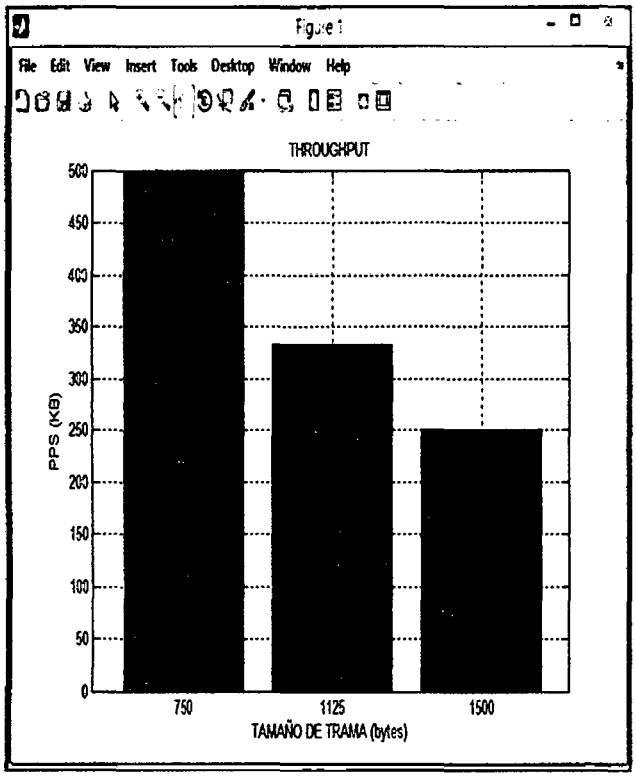


Fig. 4.6.20 PPS vs. Tamaño de Trama.

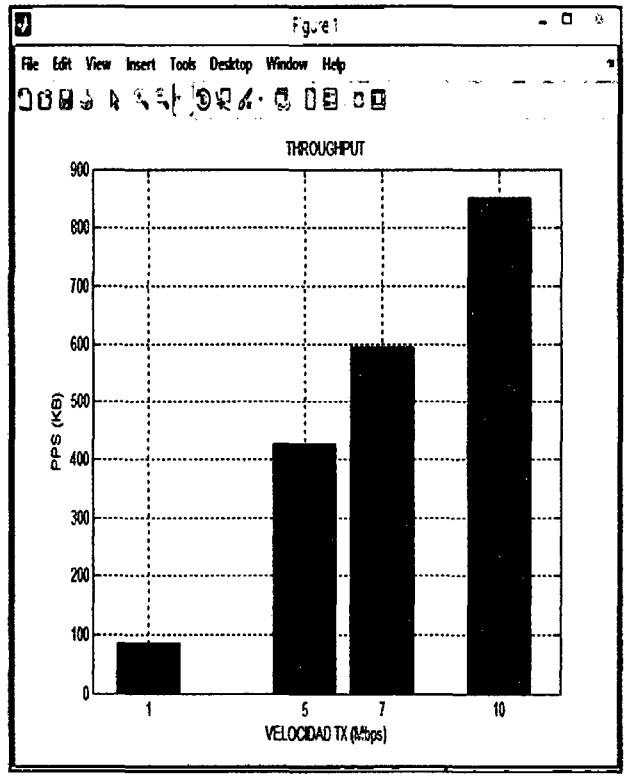


Fig. 4.6.21 PPS vs. Velocidad Tx.

En la figura 4.6.20, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 750 bytes, 1125 bytes y 1500 bytes los cuales han utilizado una velocidad de Tx constante de 0.5 Mbps, en la gráfica se puede observar claramente que al enviar una trama de 750 bytes se envía 500 pps, con una trama de 1125 se envía 333 pps y con una trama de 1500 se envía 250 pps.

Mientras en la figura 4.6.21, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 1470 bytes los cuales han utilizado una velocidad de Tx variada de: 1 Mbps, 5 Mbps, 7 Mbps y 10 Mbps, sin que se produzcan perdidas en el envío, como los datos que se muestran en la tabla 4.6.7.

PASO 3: Medición del Jitter

Para la medición se envió datos UDP de longitud variable a velocidades diferentes de Throughput obtenida anteriormente durante 20 segundos. Como se utilizó anteriormente Jperf el cliente será el encargado de enviar los datos y el servidor los recibirá, indicando los valores de Jitter obtenidos durante la transmisión de los datos.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**3**	**3**	**3**
Velocidad de Rx (Mbps)	**3**	**3**	**2.99**
Tramas Transmitidas	**4994**	**3330**	**2498**
Tramas Recibidas	**4994**	**3330**	**2498**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**0.482**	**1.011**	**1.549**

Tabla 4.6.8 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**1**	**5**	**7**	**10**
Velocidad de Rx (Mbps)	**1**	**4.97**	**6.83**	**7.24**
Tramas Transmitidas	**851**	**4247**	**5946**	**8505**
Tramas Recibidas	**851**	**4247**	**5946**	**8293**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**	**212 (2.5%)**
Jitter (ms)	**4.226**	**3.012**	**2.45**	**4.331**

Tabla 4.6.9 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

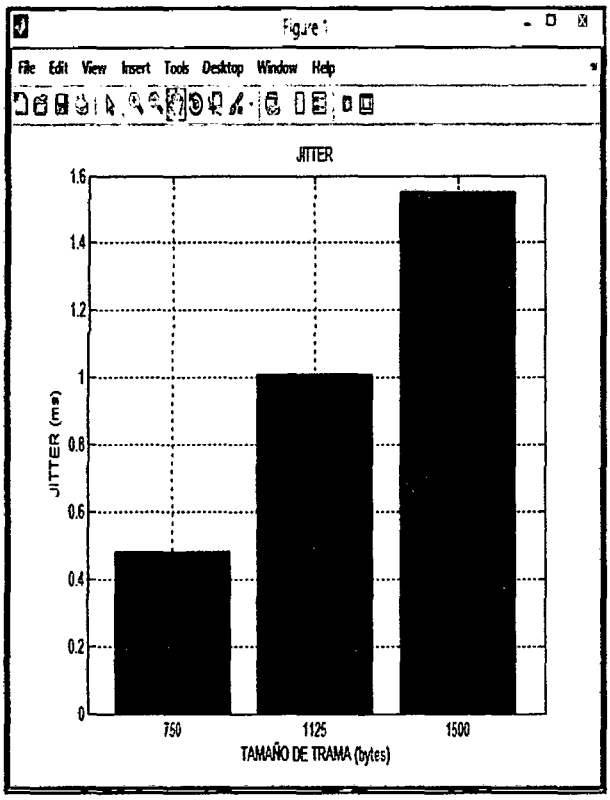


Fig. 4.6.22 Jitter vs. Tamaño de Trama

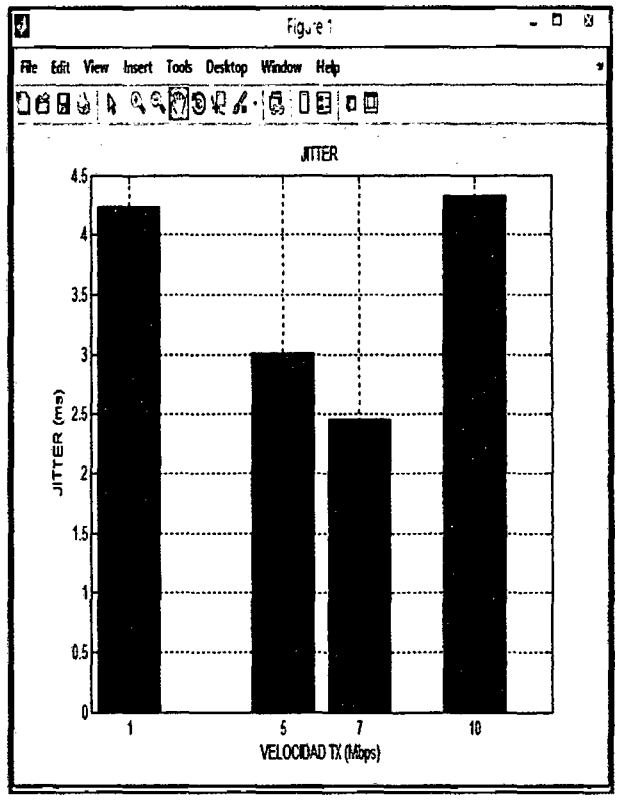


Fig. 4.6.23 Jitter vs. Velocidad Tx

En la figura 4.10.22 se observa los valores del Jitter obtenidos al enviar diferentes tamaños de paquete UDP como 750, 1125 y 1500 bytes utilizando una velocidad de Tx constante de 0.5 Mbps, se puede observar claramente que con una trama de 750 bytes se tiene un Jitter de 0.48 ms a diferencia de la trama de 1500 bytes en la cual se tiene un Jitter de 1.54 ms.

En la figura 4.10.23, se observa los valores del Jitter obtenidos al enviar paquetes UDP de 1470 bytes utilizando una velocidad de Tx que varía entre 1 Mbps, 5 Mbps y 7 Mbps sin que se pierdan paquetes en la red, concluyendo también que a mayor ancho de banda mucho mayor será el jitter y pérdidas de datagramas.

Medición de Jitter a 5 Mbps:

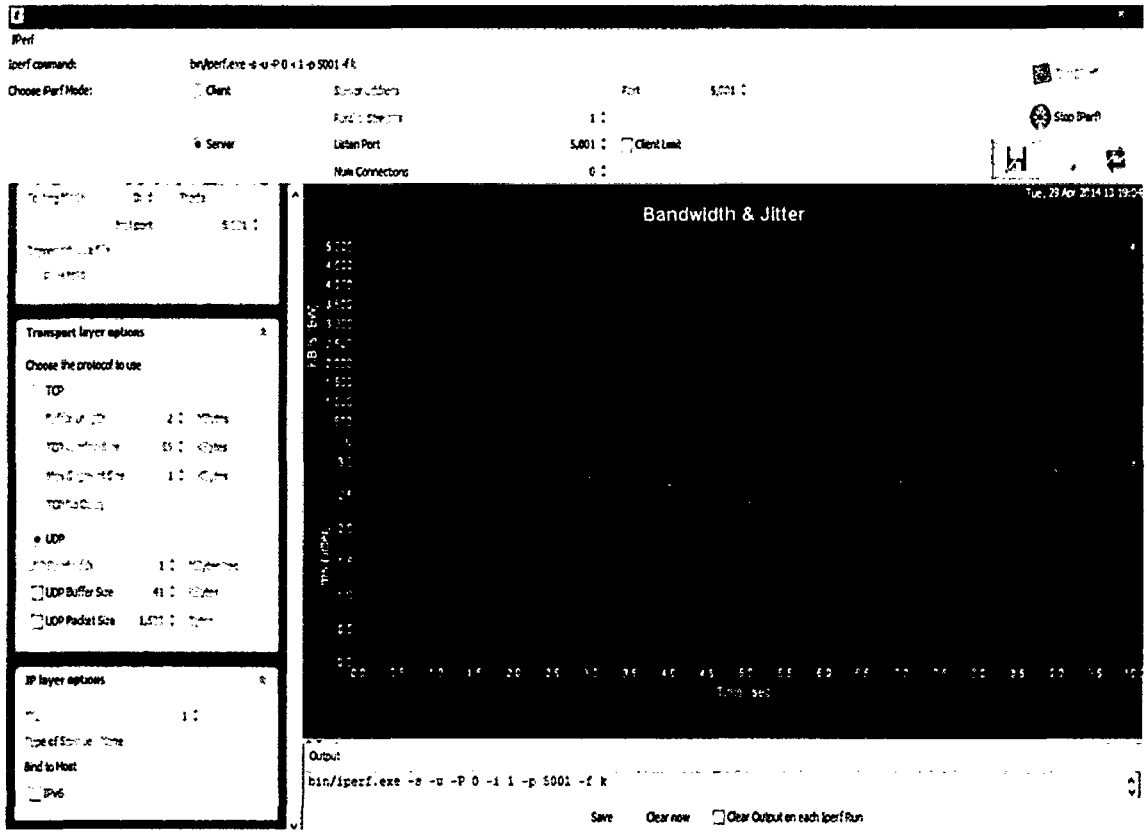


Fig. 4.6.24 Gráfica de Bandwidth y Jitter.

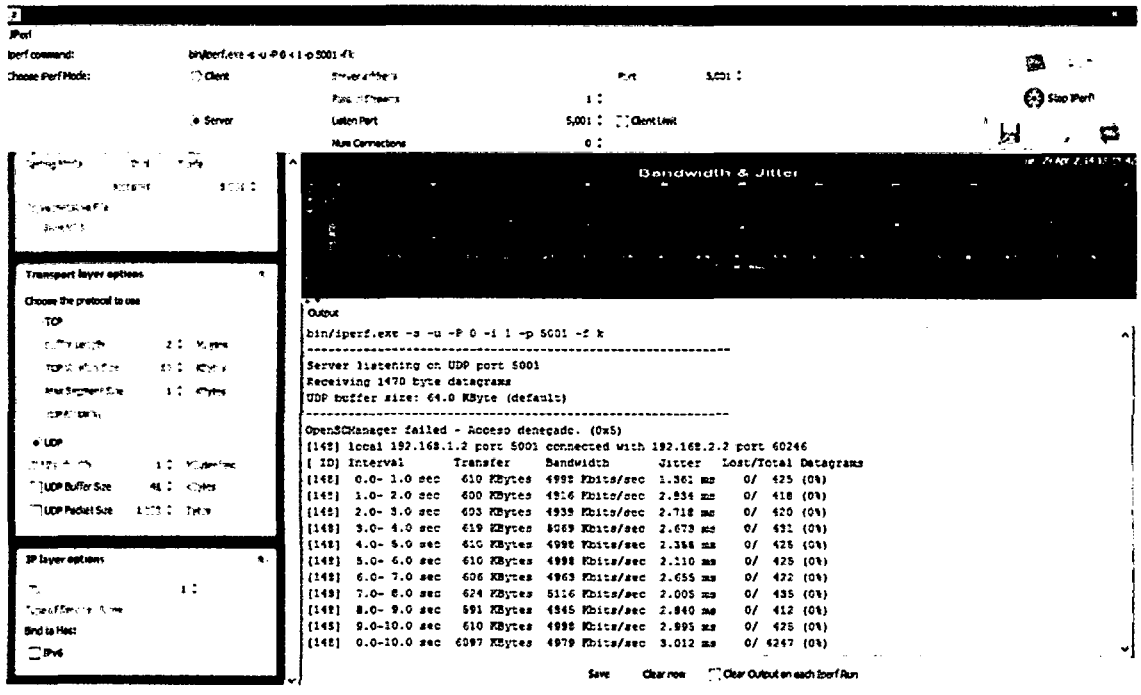


Fig. 4.6.25 Resultados al medir Throughput como servidor.

PASO 4: Captura de tráfico con Wireshark.

Capturar tráfico de paquetes en la interfaz fastethernet 1/0 de R1.

- Captura de paquetes ICMP:

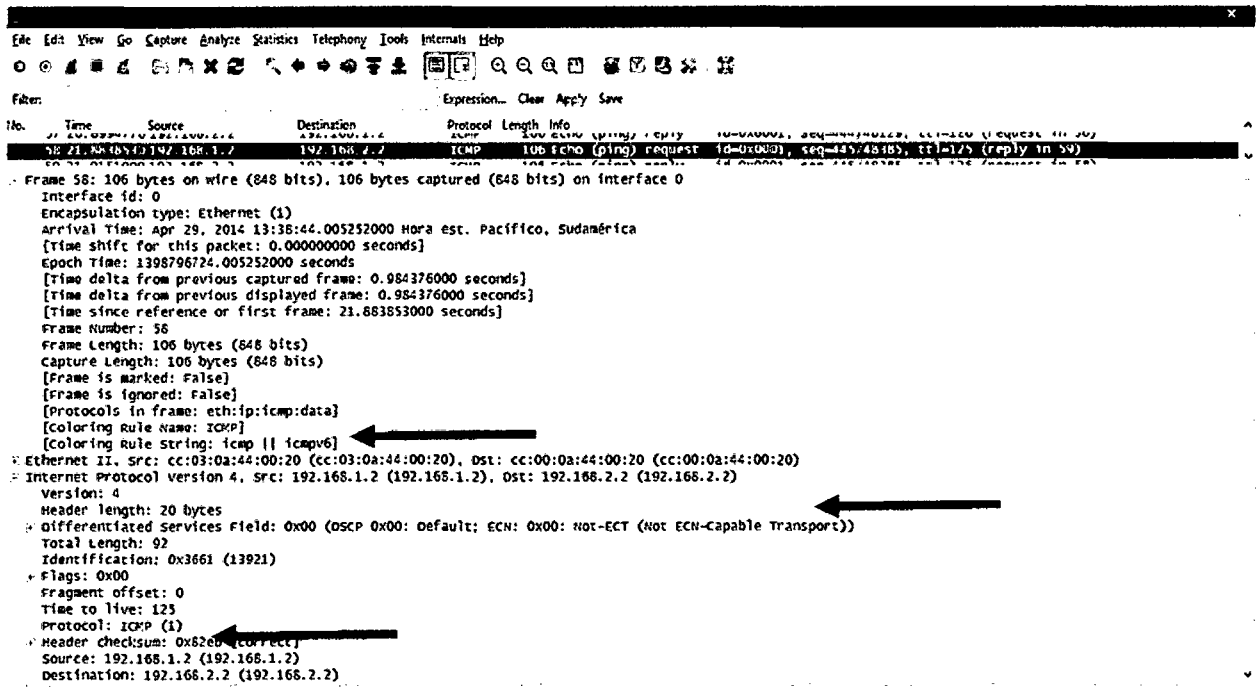


Fig. 4.6.26 Captura e información del paquete ICMP.

- Protocolo TCP, BGP lo utiliza como protocolo de transporte:

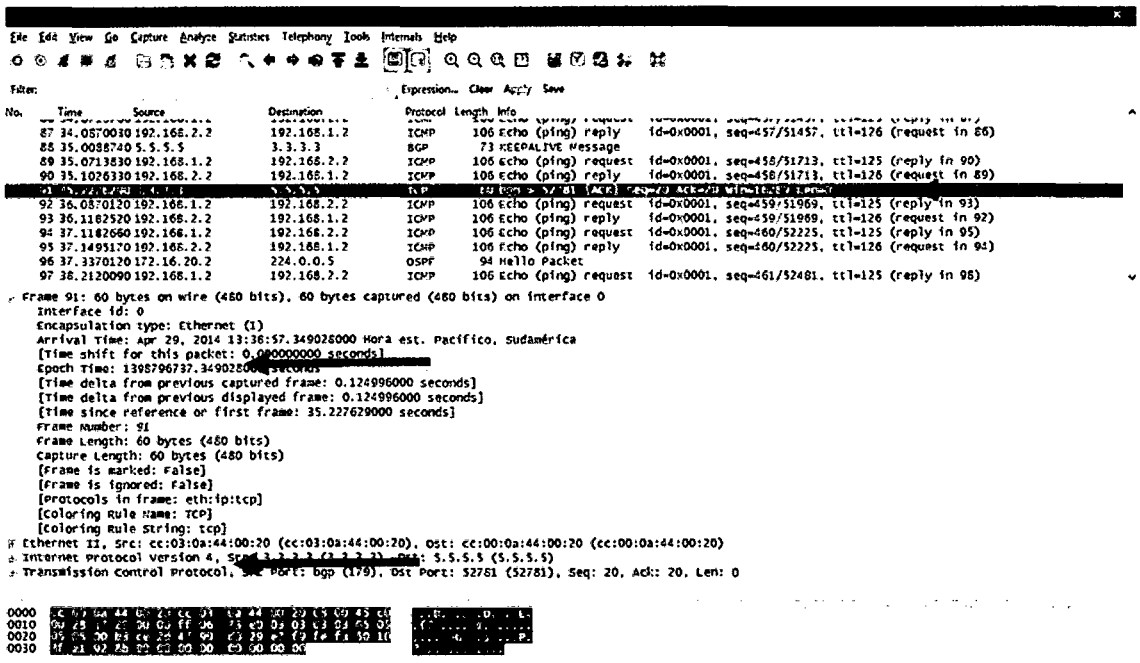


Fig. 4.6.27 Captura del protocolo TCP

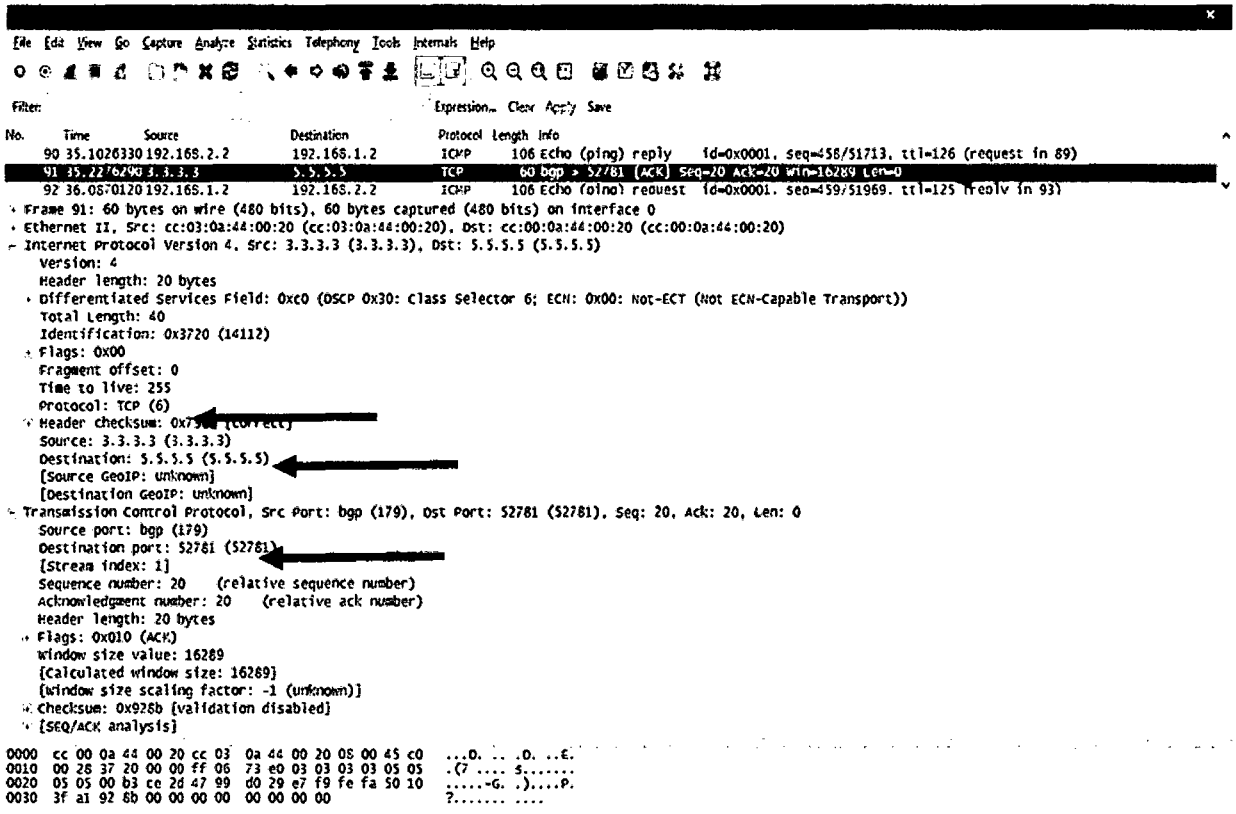


Fig. 4.6.28 Información detallada del protocolo TCP

- Protocolo BGP

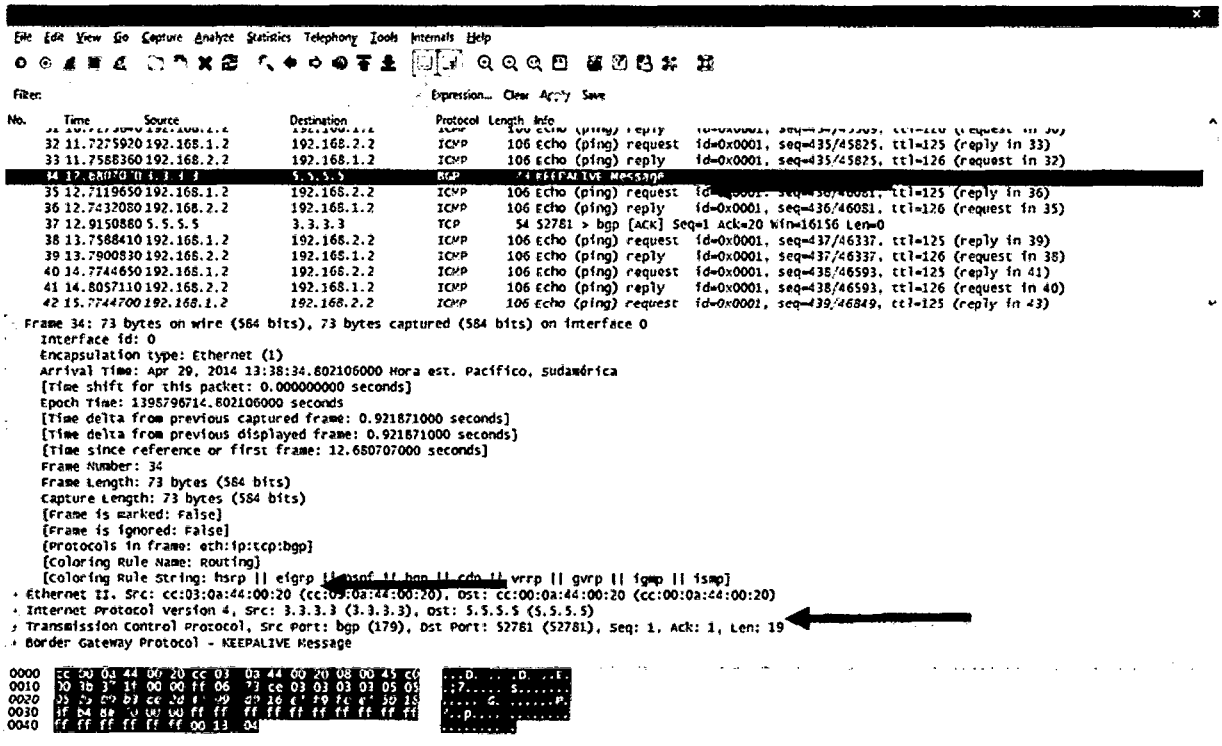


Fig. 4.6.29 Captura del protocolo BGP.

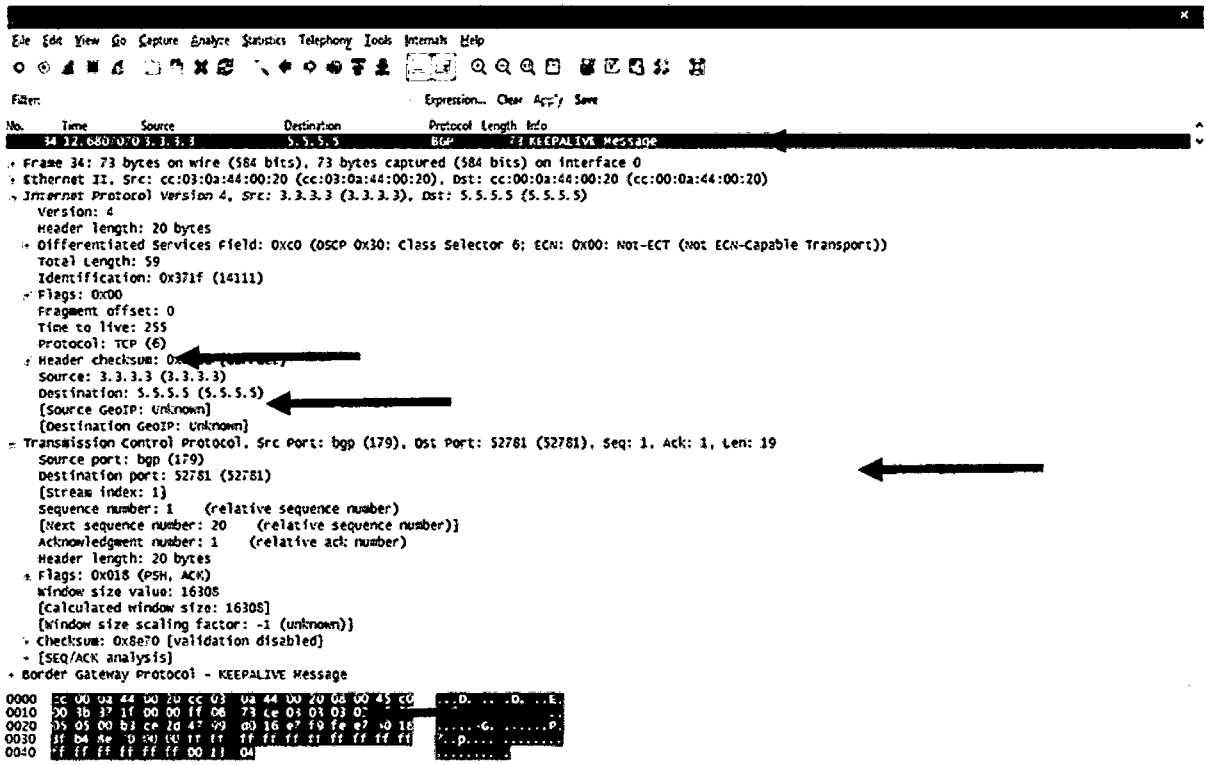


Fig. 4.6.30 Información detallada del protocolo BGP.

- Protocolo OSPF

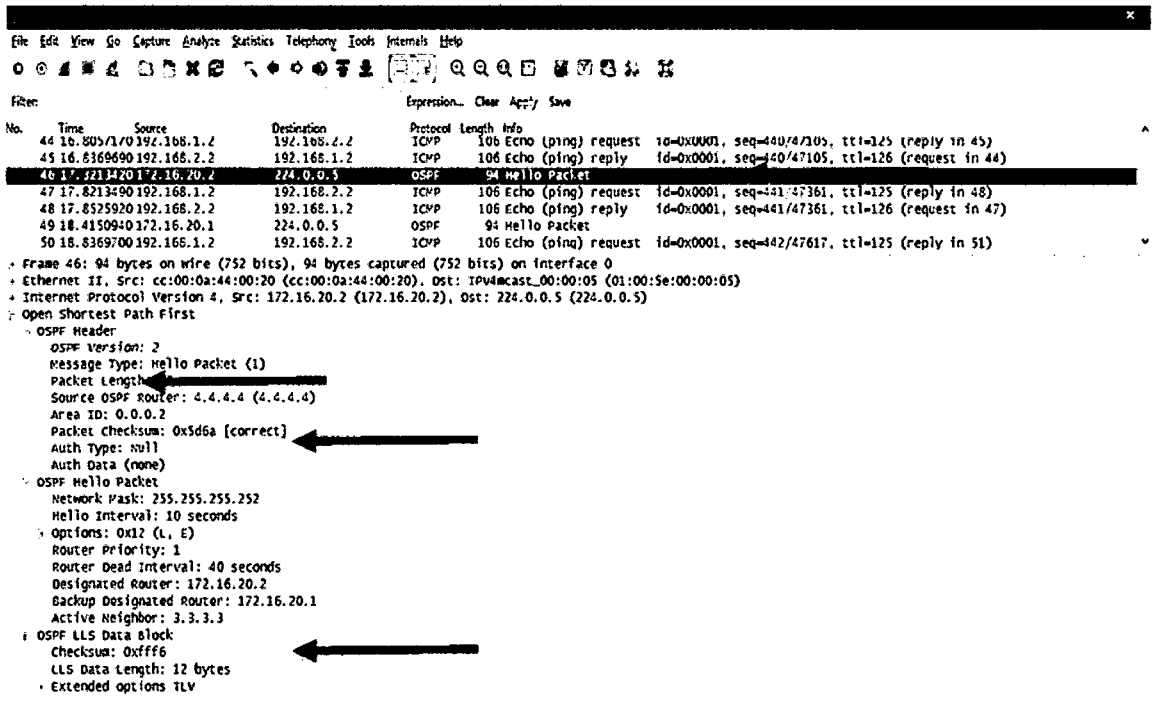


Fig. 4.6.31 Captura del protocolo OSPF.

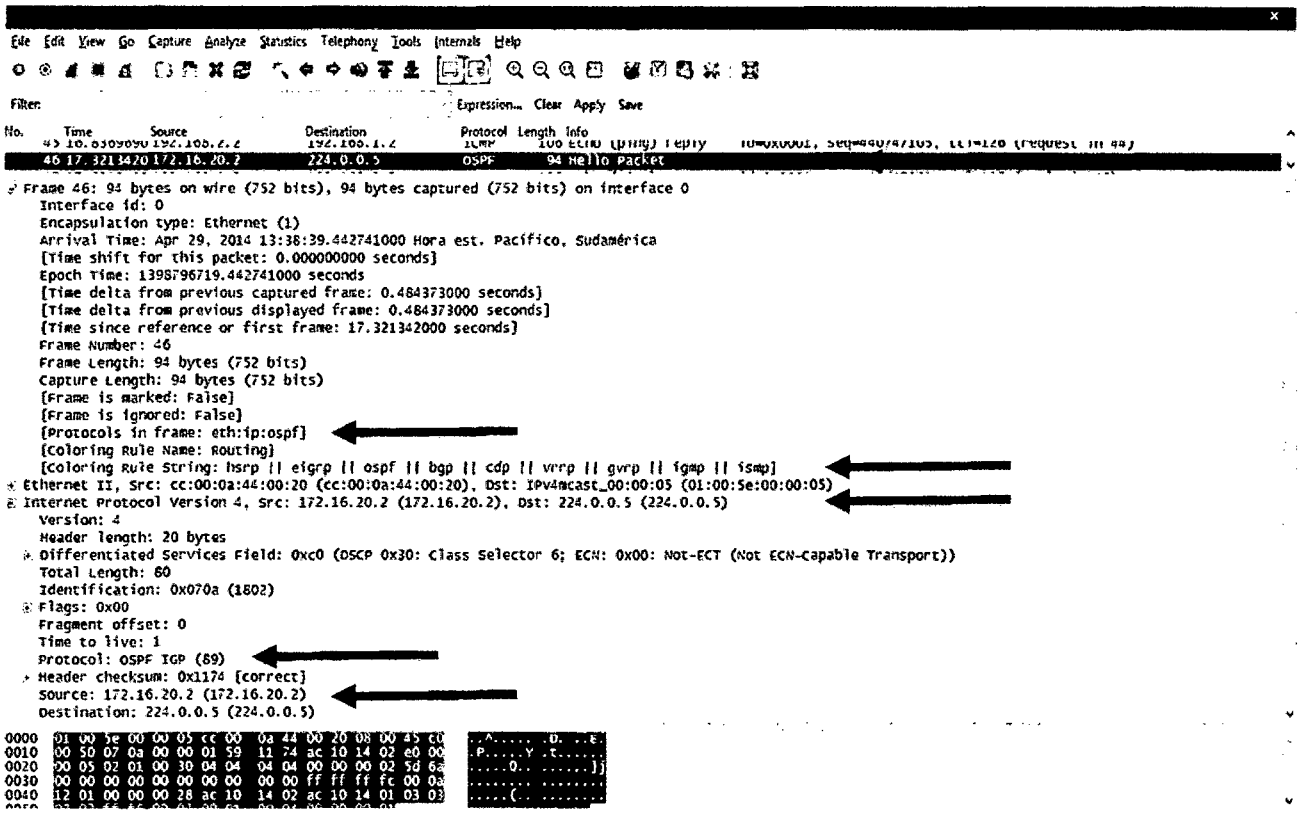


Fig. 4.6.32 Información detallada del protocolo OSPF.

LABORATORIO 4.7: CONFIGURACIÓN BASICA DE ENRUTAMIENTO INTER VLAN

REVISIÓN TEÓRICA: Para la realización de esta práctica se deberá revisar conceptos de configuración de VLAN, VTP, Enrutamiento inter VLAN.

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología.
- Borrar las configuraciones y volver a cargar un switch y un router al estado predeterminado.
- Realizar las tareas básicas de configuración en una LAN conmutada y un router.
- Configurar las VLAN y el protocolo VLAN Trunking (VTP) en todos los switches.
- Configurar un router para admitir el enlace 802.1q en una interfaz Fast Ethernet.
- Configurar un router con subinterfaces que correspondan a las VLAN configuradas.
- Configurar un router con el protocolo de enrutamiento OSPF.
- Demostrar y explicar el enrutamiento entre VLAN.

ESCENARIO:

En esta actividad de laboratorio, el usuario examinará y configurará switches con sus respectivas VLAN con sus LAN independientes. Pese a que el switch realiza funciones básicas en su estado predeterminado de manera no convencional, existe una cantidad de parámetros que un administrador de red debe modificar para garantizar una LAN segura y optimizada. Esta práctica de laboratorio se armará y conectará la red que se muestra en el Diagrama de topología teniendo en cuenta los siguientes requisitos:

Vlan 10: 240 host.

Vlan 20: 200 host.

Vlan 30: 200 host.

Vlan 40: 240 host.

Luego realice las configuraciones básicas en los routers y switch, para que se realice la comunicación entre los hosts de las vlan. Después de completar la configuración pruebe la conectividad entre los dispositivos de la red y finalmente analizará el tráfico de paquetes en dicha topología.

DIAGRAMA DE TOPOLOGÍA:

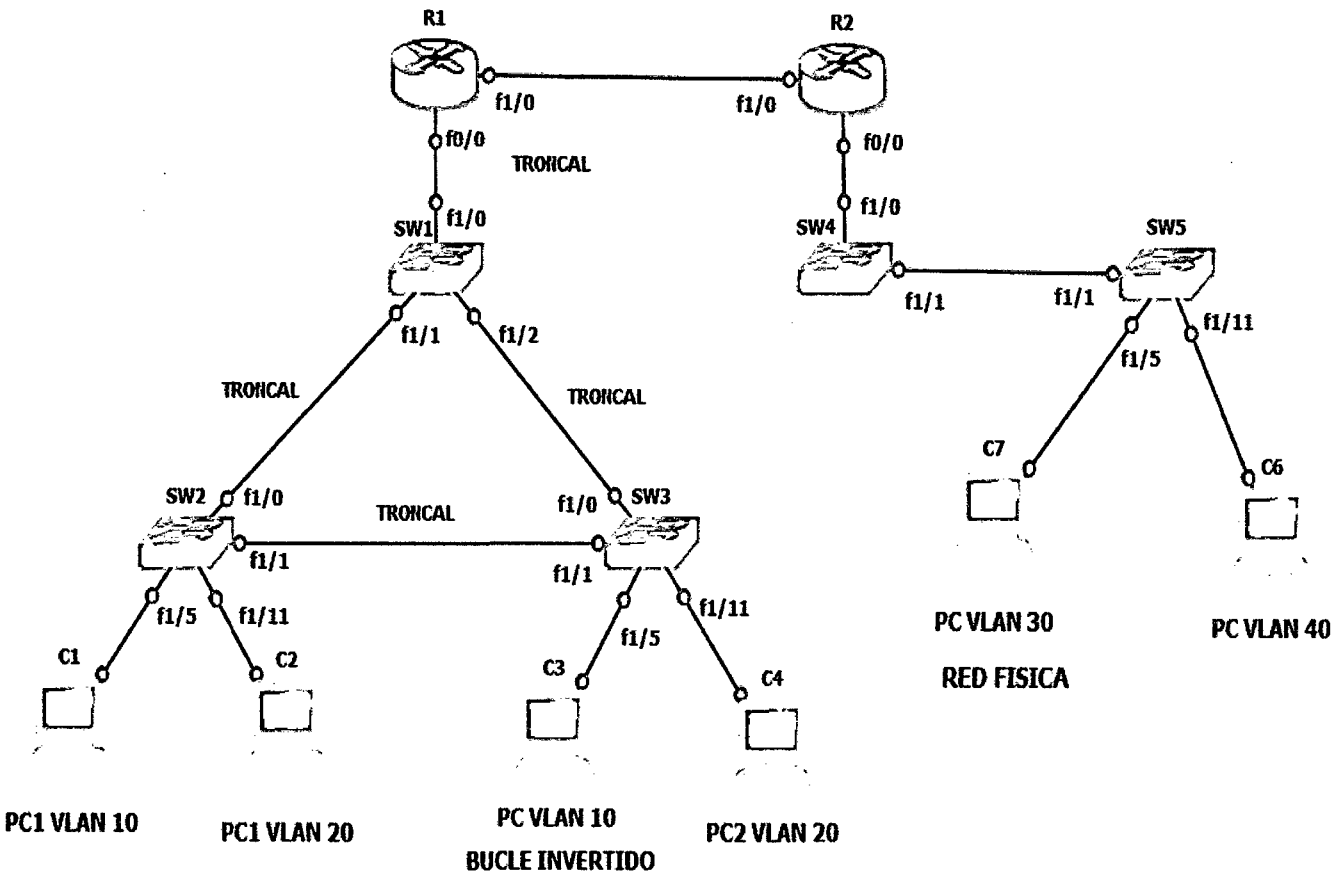


Fig. 4.7.1 Red Virtual en GNS3.

TAREA 1: MONTAR LA RED EN GNS3

PASO 1: Montar y conectar la red igual a la del Diagrama de topología.

PASO 2: Borrar toda configuración existente en los switches.

En los switches borre la NVRAM, borre el archivo vlan.dat y reinicie los switches (solo en los switch físicos). Después de que la recarga se haya completado, utilice el comando **show vlan-sw** para verificar que solo existan VLAN predeterminadas y que todos los puertos se asignen a la VLAN 1, este comando solo es para GNS3 para los switch físicos solo es el comando **show vlan.**

PASO 3: Borrar la configuración en el router y volver a cargar.

Router#**erase startup-config**

Erasing the nvram filesystem will remove all configuration files! Continue?

[confirm]

Erase of nvram: complete

Router#**reload**

System configuration has been modified. Save? [yes/no]: **no**

TAREA 2: REALICE EL DIRECCIONAMIENTO IP PARA LAS REDES LAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	f1/0	172.16.2.1	255.255.255.252	No aplicable
	f0/0.1	172.16.1.1	255.255.255.0	No aplicable
	f0/0.10	172.16.10.1	255.255.255.0	No aplicable
	f0/0.20	172.16.20.1	255.255.255.0	No aplicable
R2	f0/0	172.16.2.2	255.255.255.0	No aplicable
	f0/1.30	172.1.30.1	255.255.255.0	No aplicable
	f0/1.40	172.1.40.1	255.255.255.0	No aplicable
	f0/1.1	172.16.99.1	255.255.255.0	No aplicable
C3	BUCLE INVERTIDO	172.16.10.3	255.255.255.0	172.16.10.1
C1	VPCS	172.16.10.2	255.255.255.0	172.16.10.1
C2	VPCS	172.16.20.2	255.255.255.0	172.16.20.1
C4	VPCS	172.16.20.3	255.255.255.0	172.16.20.1
PC VLAN 30	NIC	172.16.30.2	255.255.255.0	172.16.30.1
PC VLAN 40	NIC	172.16.40.2	255.255.255.0	172.16.40.1

Tabla 4.7.1 Direccionamiento IP para las Redes.

ASIGNACIONES DE PUERTO: SW1

Puertos	Asignación	Red
f 1/0 – f 1/2	Enlaces troncales 802.1q (LAN 1 nativa)	**172.16.1.1 /24**

Tabla 4.7.2 Asignación de Puertos SW1.

ASIGNACIONES DE PUERTO: SW2

Puertos	Asignación	Red
f1/0 – f1/1	Enlaces troncales 802.1q (LAN 1 nativa)	**172.16.1.0 /24**
f1/5 – f1/10	Vlan 10	**172.16.10.0 /24**
f1/11 – f1/15	Vlan 20	**172.16.20.0 /24**

Tabla 4.7.3 Asignación de Puertos SW2.

ASIGNACIONES DE PUERTO: SW3

Puertos	Asignación	Red
f1/0 – f1/1	Enlaces troncales 802.1q (LAN 1 nativa)	**172.16.1.0 /24**
f1/5 – f1/10	Vlan 10	**172.16.10.0 /24**
f1/11 – f1/15	Vlan 20	**172.16.20.0 /24**

Tabla 4.7.4 Asignación de Puertos SW3.

ASIGNACIONES DE PUERTO: SW4

Puertos	Asignación	Red
f1/0 – f1/1	Enlaces troncales 802.1q (LAN 99 nativa)	**172.16.99.0 /24**

Tabla 4.7.5 Asignación de Puertos SW4.

ASIGNACIONES DE PUERTO: SW5

Puertos	Asignación	Red
f1/2	Enlaces troncales 802.1q (LAN 99 nativa)	**172.16.99.0 /24**
f1/5 – f1/10	Vlan 30	**172.16.30.0 /24**
f1/10 – f1/15	Vlan 40	**172.16.40.0/24**

Tabla 4.7.6 Asignación de Puertos SW5.

TAREA 3: REALIZAR LA CONFIGURACION BASICA DEL ROUTER Y SWITCHES

Una vez iniciado el equipo aparecerá el siguiente prompt:

Router>

Ingrese al modo privilegiado

Router>enable

Aparece el siguiente prompt

Router#

Switch>

Ingrese al modo privilegiado

Switch >enable

Aparece el siguiente prompt
Switch #

PASO 1: Establezca la configuración global del nombre de host.

En el modo exec privilegiado, ingrese al modo de configuración global:

Router# **configure terminal**

Switch # **configure terminal**

Ingrese el siguiente comando para configurar el nombre del router:

Router(config)#**hostname XXXXXX** (Escribir nombre deseado)

Switch(config)#**hostname XXXXXX**

PASO 2: Configure un mensaje para que se muestre al ingresar al router.

Router(config)#**banner motd %** Solo acceso a personal autorizado **%** (Puede escribir cualquier mensaje)

El símbolo % indica el inicio y final del mensaje

Switch(config)# **banner motd %** Solo acceso a personal autorizado **%**

PASO 3: Configure las contraseñas de consola, enable secret y VTY.

Seguir los siguientes pasos para el switches:

Switch(config)# **line console 0**

Switch(config-line)# **password XXXXX**

Switch(config-line)# **login**

Switch(config-line)# **exit**

Switch(config)# **enable secret XXXXX**

Switch(config)# **line vty 0 4**

Switch(config-line)# **password XXXXX**

Switch(config-line)# **login**

Switch(config-line)# **exit**

PASO 4: Desactive la búsqueda DNS.

Router(config)# **no ip-domain lookup**

Si escribes algo que no sea un comando de Cisco IOS o cometes un error, el router asume que ha escrito un nombre de dominio y trata de resolver lo que usted escribe, realizando una búsqueda de DNS.

PASO 5: Sincronice los mensajes no solicitados y el resultado de la depuración con el resultado solicitado y los indicadores para las líneas de consola y de terminal virtual.

Router(config)# **line console 0**

Router(config)# **logging synchronous**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **logging synchronous**

Router(config)# **exit**

PASO 6: Configure un tiempo de espera EXEC de 10 minutos.

Router(config)# **line console 0**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

PASO 7: Guardar la configuración.

Router(config)# **copy running-config startup-config**

NOTA: Realizar la misma programación para los router's.

TAREA 4: CONFIGURE Y ACTIVE LAS INTERFACES FASTETHERNET.

Aplique Los siguientes comandos:

R1:

Configuración para una interface fasEthernet:

R1(config)# **interface fasEthernet 1/0**

R1(config-if)# **description conexion a R2**

R1(config-if)# **ip address 172.16.2.1 255.255.255.252**

R1(config-if)# **no shutdown**

R1(config-if)# **end**

R2:

Configuración para una interface fastEthernet:

R2(config)# **interface fastEthernet 1/0**

R2(config-if)# **description conexion a R1**

R2(config-if)# **ip address 172.16.2.2 255.255.255.252**

R2(config-if)# **no shutdown**

R2(config-if)# **end**

TAREA 5: CONFIGURAR VTP EN LOS SWITCHES

Configurar VTP en los cinco switches, recuerde que las contraseñas y los nombres de dominios VTP distinguen entre mayúsculas y minúsculas.

SW4:

SW4(config)#**vtp mode server**

SW4(config)#**vtp domain unprg**

SW4(config)#**vtp password unprg**

SW5:

SW5(config)#**vtp mode client**

SW5(config)#**vtp domain unprg**

SW5(config)#**vtp password unprg**

SW1:

SW1# **vlan database**

SW1(vlan)# **vtp server**

SW1(vlan)# **vtp domain unprg**

SW1(vlan)# **vtp password unprg**

SW2:

SW2# **vlan database**

SW2(vlan)# **vtp client**

SW2(vlan)# **vtp domain unprg**

SW2(vlan)# **vtp password unprg**

SW3:

SW3# **vlan database**

SW3(vlan)# **vtp client**

SW3(vlan)# **vtp domain unprg**

SW3(vlan)# **vtp password unprg**

TAREA 6: CONFIGURAR LAS VLAN EN EL SERVIDOR VTP.

PASO 1: Configure las siguientes VLAN en los servidores VTP:

SW1:

Vlan	Nombre de la Vlan
Vlan 10	Vlan-estudiantes-centropre
Vlan 20	Vlan-docentes-centropre

Tabla 4.7.7 Nombre de VLAN en SW1.

SW4:

Vlan	Nombre de la Vlan
Vlan 99	Vlan-administracion
Vlan 30	Vlan-estudiantes
Vlan 40	Vlan-docentes

Tabla 4.7.8 Nombre de VLAN en SW4.

SW4:

SW4(config)#**vlan 99**

SW4(config-vlan)#**name vlan-administracion**

SW4(config-vlan)#**exit**

SW4(config)#**vlan 30**

SW4(config-vlan)#**name vlan-estudiantes**

SW4(config-vlan)#**exit**

SW4(config)#**vlan 40**

SW4(config-vlan)#**name vlan-docentes**

SW4(config-vlan)#**exit**

SW1:

SW1# **vlan database**

SW1(vlan)# **vlan 10 name vlan-estudiantes-centropre**

SW1(vlan)# **vlan 20 name vlan-docentes-centropre**

SW1(vlan)#**exit**

PASO 2: Configurar los puertos de enlace troncales y designar la VLAN nativa para los enlaces troncales.

Configure Fa0/23 y Fa0/24 como puertos de enlace troncales y designe la VLAN 99 como la VLAN nativa para estos enlaces troncales. Simplifique esta tarea con el comando interface **range** en el modo de configuración global.

SW4:

SW4(config)#**interface range fa0/0- 1**

SW4(config-if-range)#**switchport mode trunk**

SW4(config-if-range)#**switchport trunk native vlan 99**

SW4(config-if-range)#**no shutdown**

SW4(config-if-range)#**end**

SW5:

SW5(config)# **interface fa0/1**

SW5(config-if)#**switchport mode trunk**

SW5(config-if)#**switchport trunk native vlan 99**

SW5(config-if)#**no shutdown**

SW5(config-if)#**end**

Configure Fa1/0, Fa1/1 y Fa1/2 como puertos de enlace troncales.

SW1:

SW1(config)# **interface range fasEthernet 1/0 – 2**

SW1(config-if-range)#**switchport mode trunk**

SW1(config-if)# **exit**

SW2:

SW2(config)# **interface range fasEthernet 1/0 – 1**

SW2(config-if-range)#**switchport mode trunk**

SW2(config-if)# **exit**

SW3:

SW3(config)# **interface range fasEthernet 1/0 - 1**

SW3(config-if-range)#**switchport mode trunk**

SW3(config-if)# **exit**

PASO 3: Configurar la dirección de la interfaz de administración en los tres switches.

SW4(config)#**interface vlan 99**

SW4(config-if)#**ip address 172.16.99.11 255.255.255.0**

SW4(config-if)#**no shutdown**

SW5(config)#**interface vlan 99**

SW5(config-if)#**ip address 172.16.99.12 255.255.255.0**

SW5(config-if)#**no shutdown**

PASO 4: Asignar puertos de los switches a las VLAN.

Consulte la tabla de asignación de puertos al principio del laboratorio para asignar puertos a las VLAN.

SW5:

SW5(config)#**interface range fa0/5 - 9**

SW5(config-if-range)#**switchport access vlan 30**

SW5(config-if-range)#**switchport mode access**

SW5(config-if-range)#**interface range fa0/10 - 15**

SW5(config-if-range)#**switchport mode access**

SW5(config-if-range)#**switchport access vlan 40**

SW5(config-if-range)#**end**

SW5#**copy running-config startup-config**

SW2:

SW2(config)#**interface range fa 1/5 - 9**

SW2(config-if-range)#**switchport mode access**

SW2(config-if-range)#**switchport access vlan 10**

SW2(config-if-range)#**interface range fa 1/10 - 15**

SW2(config-if-range)#**switchport mode access**

SW2(config-if-range)#**switchport access vlan 20**

SW2(config-if-range)#**end**

SW2#**copy running-config startup-config**

SW3:

SW3(config)#**interface range fa 1/5 – 9**

SW3(config-if-range)#**switchport mode access**

SW3(config-if-range)#**switchport access vlan 10**

SW3(config-if-range)#**interface range fa 1/10 – 15**

SW3(config-if-range)#**switchport mode access**

SW3(config-if-range)#**switchport access vlan 20**

SW3(config-if-range)#**end**

SW3#**copy running-config startup-config**

TAREA 7: CONFIGURAR LA INTERFAZ DE ENLACES TRONCALES EN R1 Y R2.

Ha demostrado que la conectividad entre las VLAN requiere enrutamiento en la capa de la red, exactamente igual que la conectividad entre dos redes remotas cualesquiera.

Un enfoque alternativo es crear una o más conexiones Fast Ethernet entre el dispositivo L3 (el router) y el switch de capa de distribución, y configurar estas conexiones como enlaces troncales dot1q. Esto permite que el tráfico entre las VLAN sea transportado a y desde el dispositivo de enrutamiento en un solo enlace troncal. Sin embargo, requiere que la interfaz L3 sea configurada con múltiples direcciones IP. Esto puede hacerse creando interfaces 'virtuales', llamadas subinterfaces, en uno de los puertos del router Fast Ethernet y configurándolos para que reconozcan la encapsulación dot1q.

Emplear el enfoque de configuración de subinterfaces requiere de los siguientes pasos:

- Ingresar al modo de configuración de subinterfaz.
- Establecer encapsulamiento de enlace troncal.
- Asociar la VLAN con la subinterfaz.
- Asignar una dirección IP desde la VLAN a la subinterfaz.

Los comandos son los siguientes:

R1(config)# **subinterface fasEthernet 0/0.10**

R1(config-subif)# **encapsulation dot1Q 10**

R1(config-subif)# **ip address 172.16.10.1 255.255.255.0**

R1(config-subif)# **exit**

R1(config)# **subinterface fasEthernet 0/0.20**

R1(config-subif)# **encapsulation dot1Q 20**

R1(config-subif)# **ip address 172.16.20.1 255.255.255.0**

R1(config-subif)# **exit**

R1(config)# **interface fasEthernet 0/0**

R1(config-if)# **no shutdown**

R1(config-if)# **end**

R2(config)# **interface fastEthernet 0/1.30**

R2(config-subif)# **encapsulation dot1Q 30**

R2(config-subif)# **ip address 172.16.30.1 255.255.255.0**

R2(config-subif)# **exit**

R2(config)# **interface fastEthernet 0/1.40**

R2(config-subif)# **encapsulation dot1Q 40**

R2(config-subif)# **ip address 172.16.40.1 255.255.255.0**

R2(config-subif)# **exit**

R2(config-if)#**interface fastethernet 0/1.99**

R2(config-subif)#**encapsulation dot1q 99 native**

R2(config-subif)#**ip address 172.16.99.1 255.255.255.0**

R2(config-subif)# **exit**

R2(config)# **interface fastEthernet 0/1**

R2(config-if)# **no shutdown**

R2(config-if)# **end**

TAREA 8: CONFIGURE EL OSPF EN EL ROUTER R1 Y R2.

R1(config)#**router ospf 1**
R1(config-router)#**network 172.16.2.0 0.0.0.3 area 0**
R1(config-router)#**network 172.16.10.0 0.0.0.255 area 0**
R1(config-router)#**network 172.16.20.0 0.0.0.255 area 0**
R1(config-router)#**end**
R1#**copy run start**

R2(config)#**router ospf 1**
R2(config-router)#**network 172.16.2.0 0.0.0.3 area 0**
R2(config-router)#**network 172.16.30.0 0.0.0.255 area 0**
R2(config-router)#**network 172.16.40.0 0.0.0.255 area 0**
R2(config-router)#**network 172.16.99.0 0.0.0.255 area 0**
R2(config-router)#**end**
R2#**copy run start**

TAREA 9: CONFIGURE DHCP EN LOS ROUTERS R1 Y R2.

R1:

R1(config)#**ip dhcp pool VLAN-DOCENTES**
R1(dhcp-config)#**network 172.16.20.0 255.255.255.0**
R1(dhcp-config)#**default-router 172.16.10.1**
R1(dhcp-config)#**dns-server 200.48.225.130**
R1(dhcp- config)#**exit**
R1(config)#**ip dhcp excluded-address 172.16.20.1**

R1(config)#**ip dhcp pool VLAN-ESTUDIANTES**
R1(dhcp-config)#**network 172.16.10.0 255.255.255.0**
R1(dhcp-config)#**default-router 172.16.10.1**
R1(dhcp-config)#**dns-server 200.48.225.130**
R1(dhcp-config)#**exit**
R1(config)# **ip dhcp excluded-address 172.16.10.1**

R2:

R2(config)#**ip dhcp pool VLAN-DOCENTES-CENTROPRE**
R2(dhcp-config)#**network 172.16.40.0 255.255.255.0**
R2(dhcp-config)#**default-router 172.16.40.1**
R2(dhcp-config)#**dns-server 200.48.225.130**
R2(dhcp- config)#**exit**
R2(config)#**ip dhcp excluded-address 172.16.40.1**

R2(config)#**ip dhcp pool VLAN-ESTUDIANTES-CENTROPRE**
R2(dhcp-config)#**network 172.16.30.0 255.255.255.0**
R2(dhcp-config)#**default-router 172.16.30.1**
R2(dhcp-config)#**dns-server 200.48.225.130**
R2(dhcp-config)#**exit**
R2(config)# **ip dhcp excluded-address 172.16.30.1**

TAREA 10: CONFIGURAR LOS EQUIPOS DE HOST.

Configurar las direcciones IP y gateways por defecto como se indican en la tabla de direccionamiento de las interfaces Ethernet de C3, C1, C2, C4, C6 (VPCS) y PC REAL para el correcto funcionamiento de dhcp.

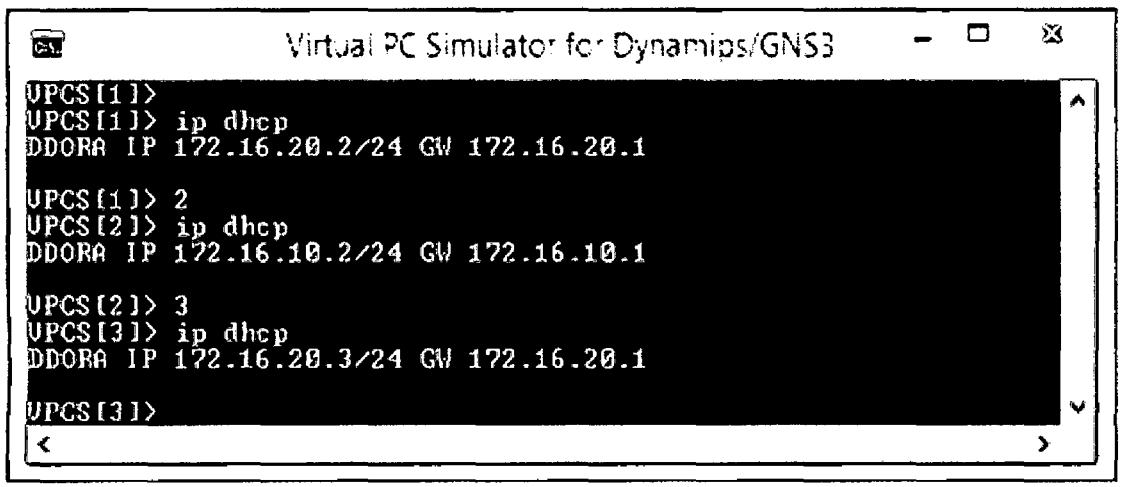


Fig. 4.7.2 Configuración de DHCP en las VPCS

TAREA 11: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

PASO 1: Verificar la configuración de VTP.

SW1**#show vtp status**

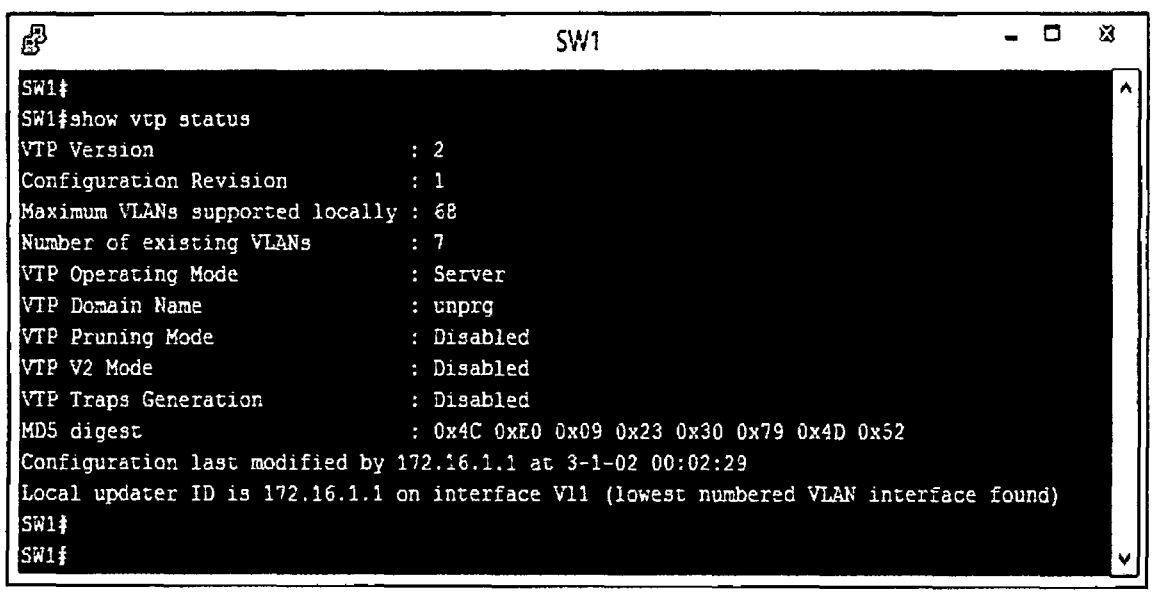


Fig. 4.7.3 Verificación de configuración de VTP en SW1

SW2#show vtp status

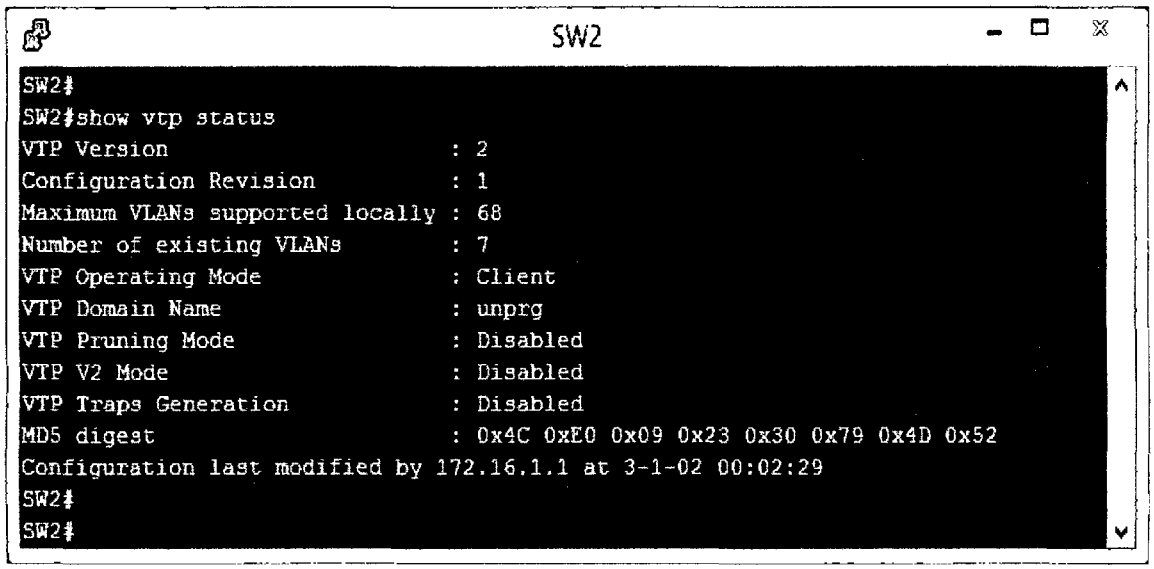


Fig. 4.7.4 Verificación de configuración de VTP en SW2

NOTA: Verificar en los demás switch la configuración vtp.

PASO 2: Verificar la creación de las VLAN en switchs y su correcta distribución a otros switch.

Use el comando **show vlan brief** en SW1 y SW4 y **show vlan-sw brief** en SW2 y SW3 para verificar que las VLAN se hayan distribuido a los switches clientes.

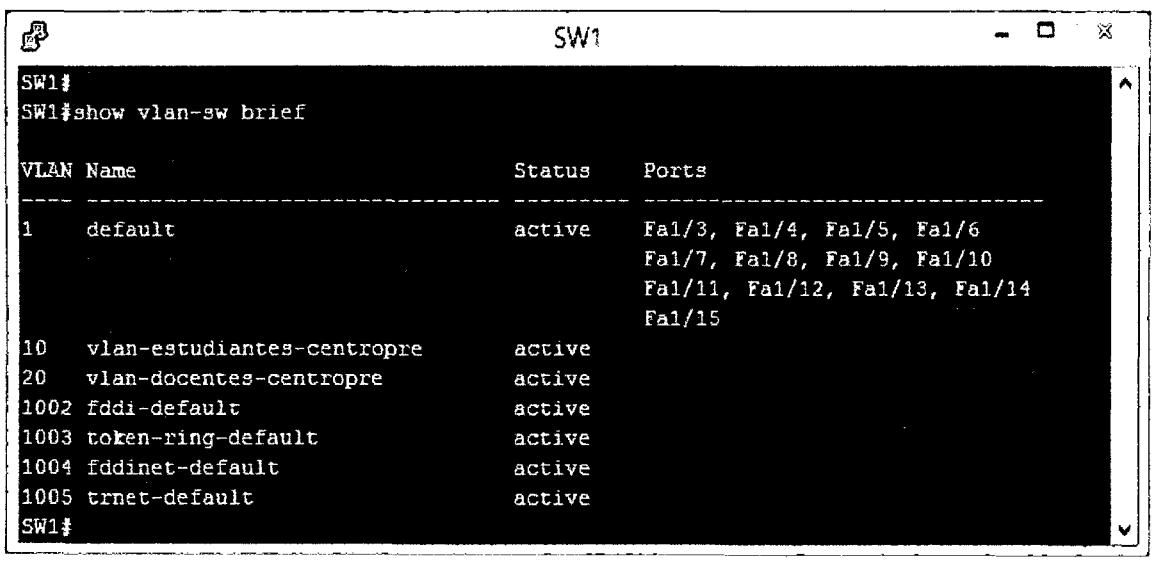


Fig. 4.7.5 Verificación de VLAN creadas.

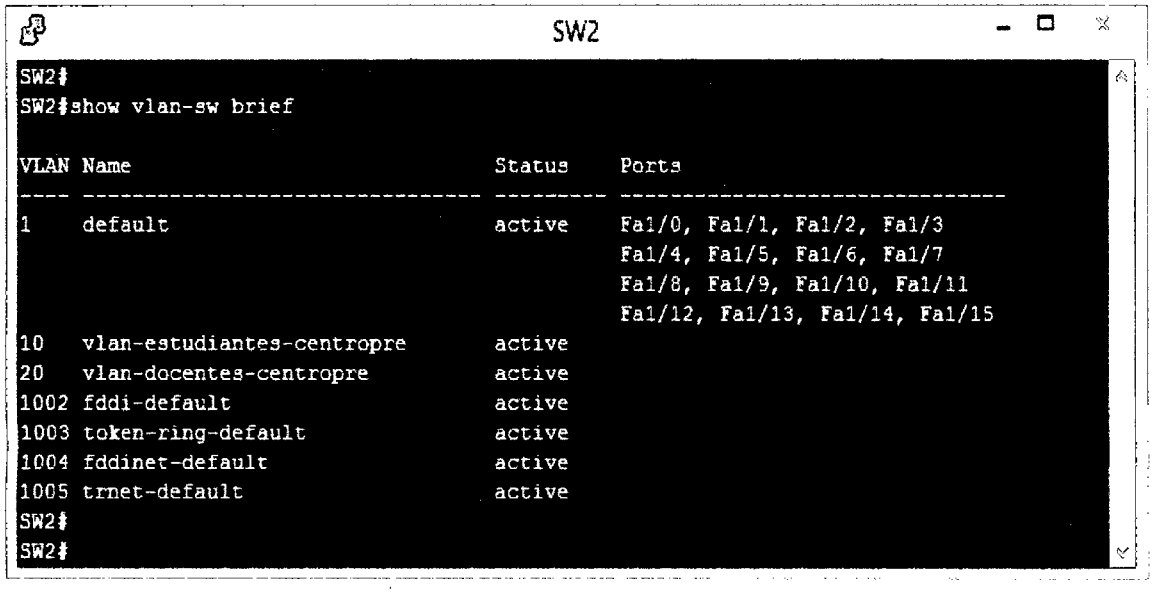


Fig. 4.7.6 Verificación de distribución de VLAN creadas.

PASO 3: Verificar el direccionamiento IP y las interfaces.

Observe los siguientes puntos en esta configuración:

- La interfaz física se habilita usando el comando no shutdown porque las interfaces de los router están inactivas de manera predeterminada. Las interfaces virtuales están activas de manera predeterminada.
- La subinterfaz puede usar cualquier número que pueda describirse con 32 bits, pero es buen ejercicio asignar el número de la VLAN como el número de la interfaz, como se hizo aquí.

- La VLAN nativa está especificada en el dispositivo L3 a fin de que sea consistente con los switches. De lo contrario, la VLAN 1 sería la VLAN nativa predeterminada, y no habría comunicación entre el router y la VLAN de administración en los switches.

R1#**show ip interface brief**

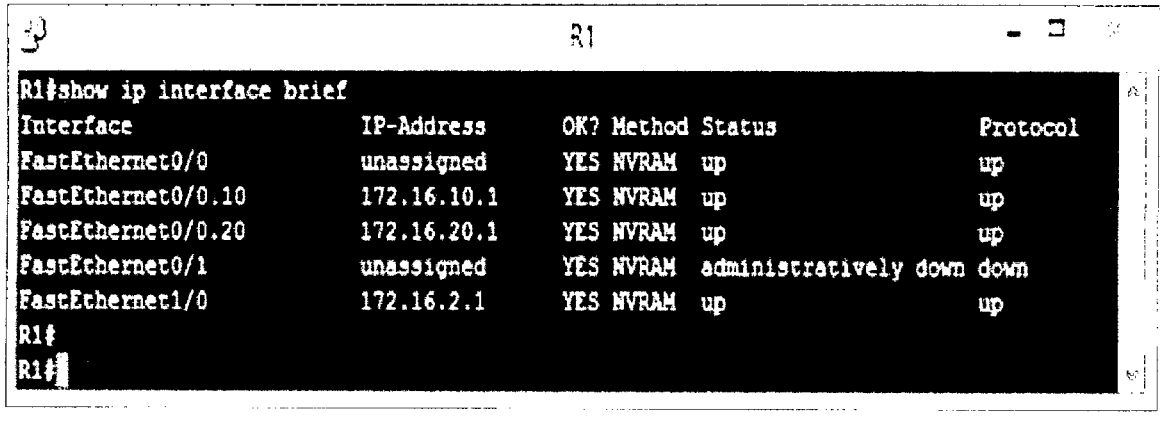


Fig. 4.7.7 Verificación de Interfaces Activas de R1

R2#show ip interface brief

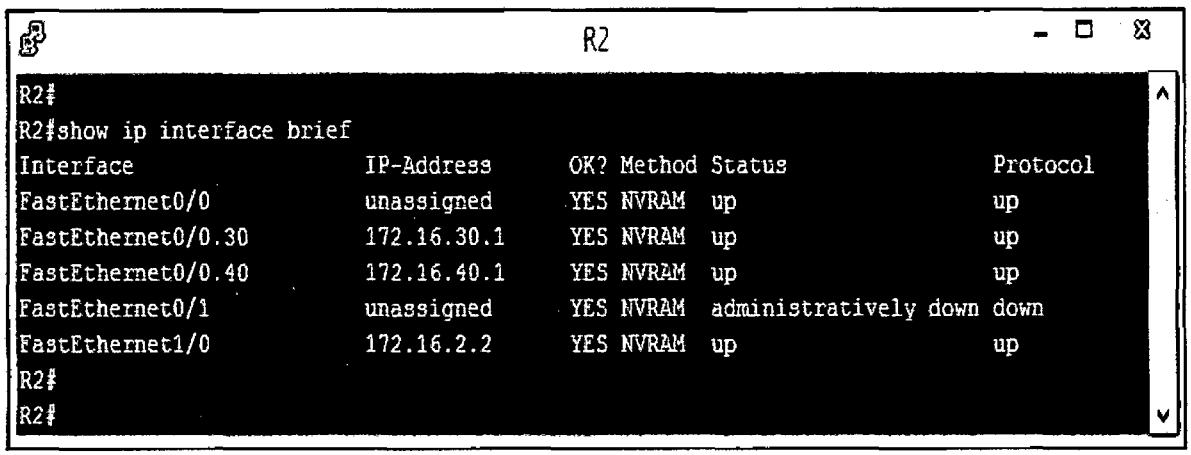


Fig. 4.7.8 Verificación de Interfaces Activas de R2

PASO 4: Verificar la configuración de los router. Use los comandos **show ip route** para verificar el contenido de la tabla de enrutamiento.

R1#show ip route

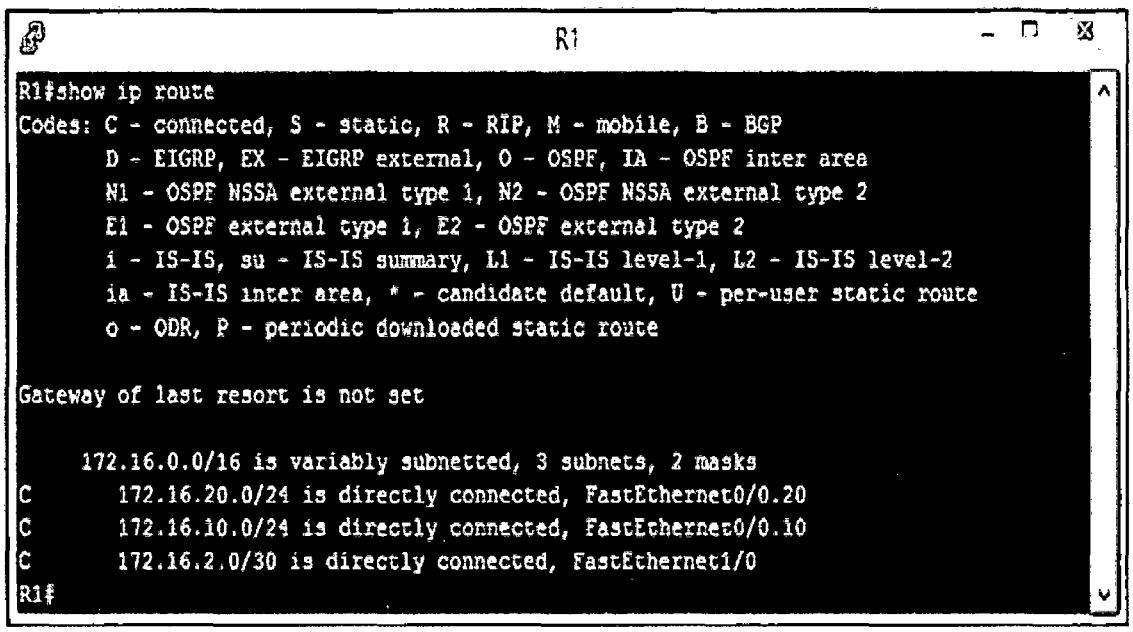


Fig. 4.7.9 Tabla de enrutamiento en R1 antes de configurar OSPF.

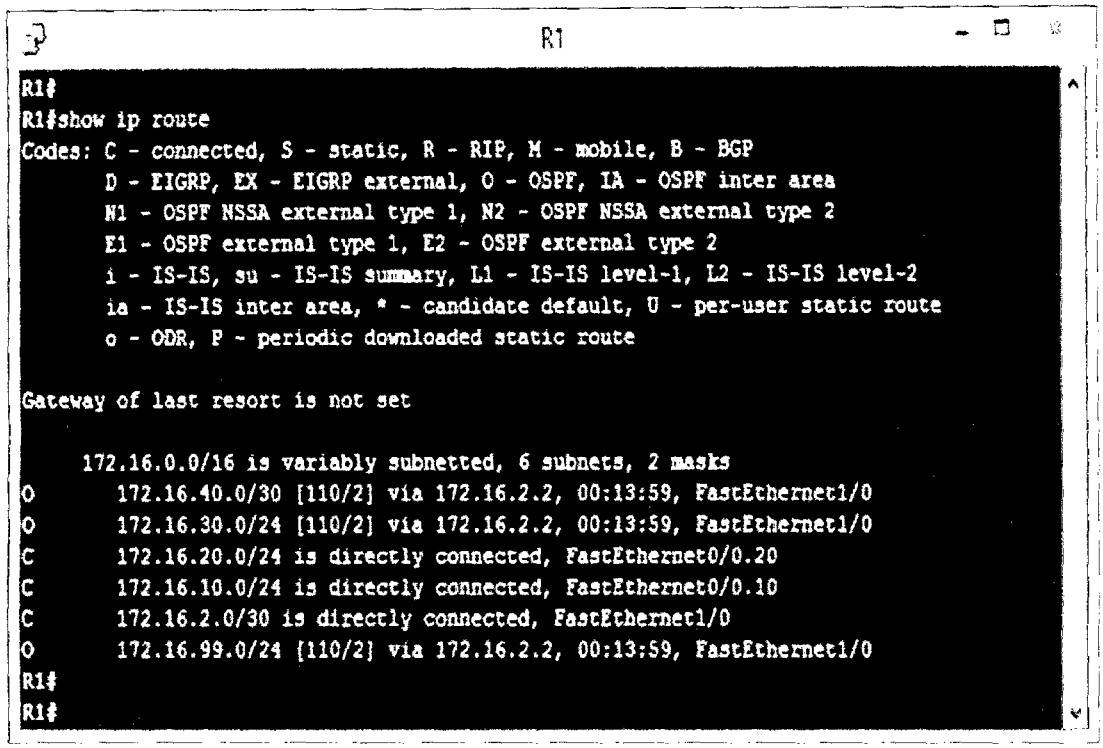


Fig. 4.7.10 Tabla de enrutamiento en R1 con OSPF.

NOTA: Verificar la table de enrutamiento de R2.

PASO 5: Verificar que hay conectividad completa en la red.

Use el comando **ping** para verificar la conectividad.

Desde la C1, verifique que pueda hacer ping a la PC real de la vlan30 y en los otros hosts. Puede que tome un par de pings antes de que se establezca la ruta de extremo a extremo.

Verifique que todos los switches estén correctamente configurados haciendo ping entre ellos.

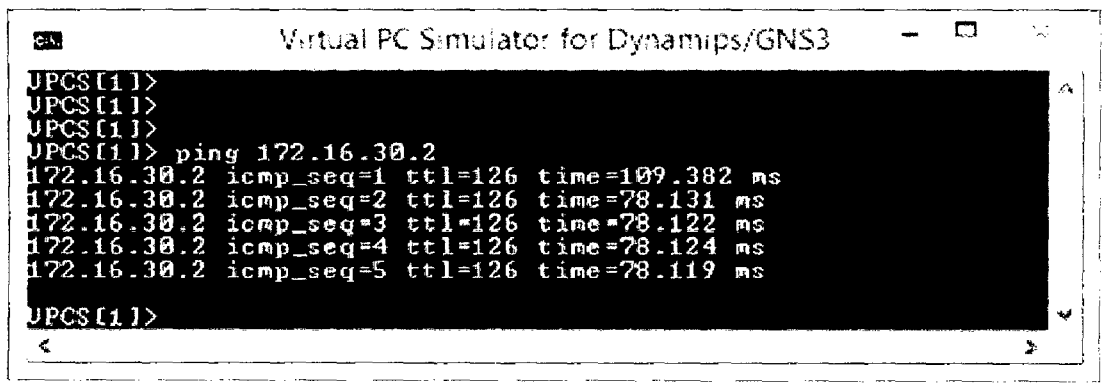


Fig. 4.7.11 Comprobación de conectividad entre C1 y PC REAL.

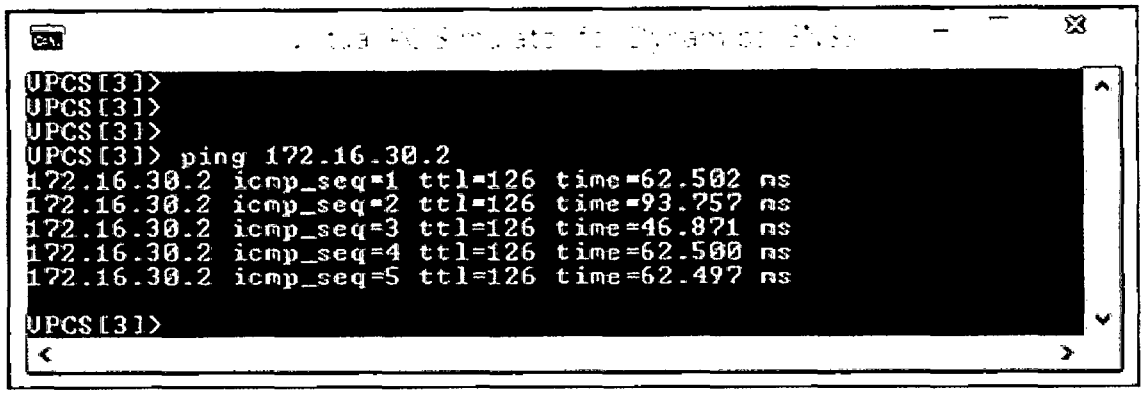


Fig. 4.7.12 Comprobación de conectividad entre C4 y PC REAL.

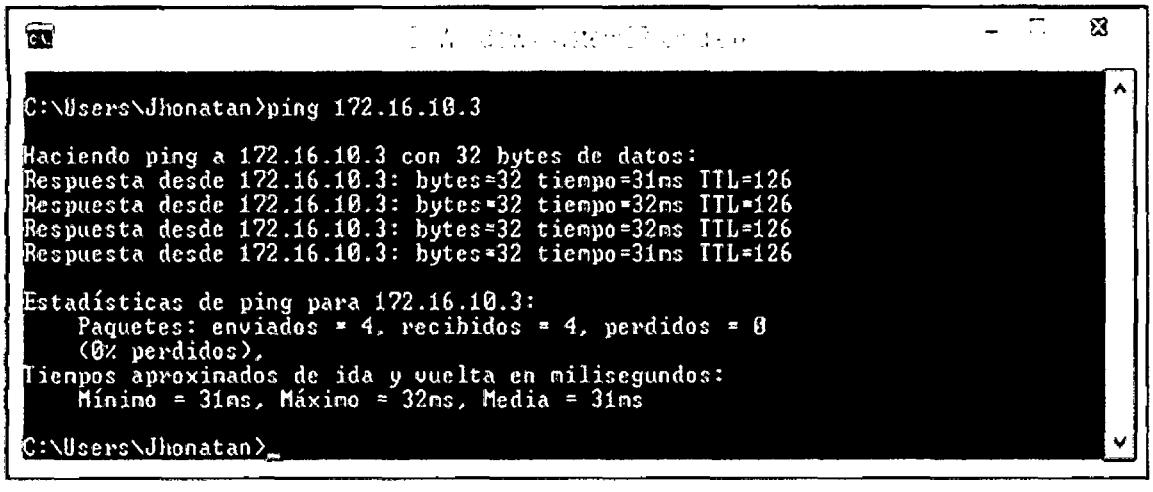


Fig. 4.7.13 Comprobación de conectividad entre PC REAL y C3.

TAREA 12: ANALIS DEL TRAFICO DE PAQUETES

PASO 1: Medición de la Latencia

Para la medición de la latencia se realizó 10 muestras sucesivas de 100 ping desde el C2 (Bucle invertido) hacia la PC REAL considerando un tamaño de trama de 64, 512 y 1518 bytes como se especifica en el RFC 2544.

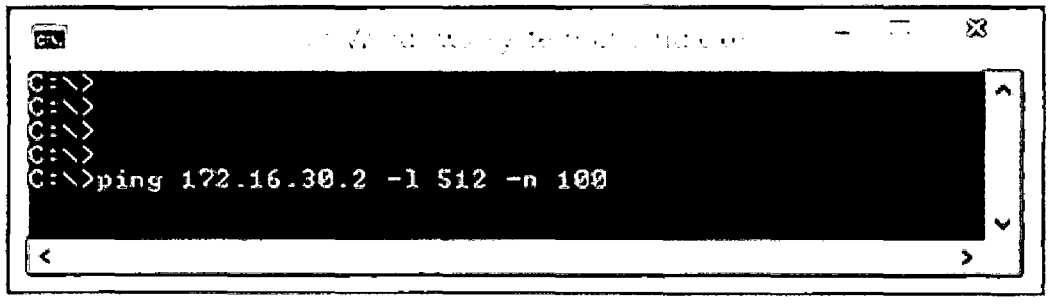


Fig. 4.7.14 Forma de medición de la Latencia.

En la Figura 4.7.14 se puede observar el envío de 100 ping con una trama de 512 hacia la dirección 172.16.30.2

En las Tablas posteriores se detallan los valores de la Latencia que se ha obtenido una vez realizadas todas las muestras.

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	**20**	**22**	**25**	**22**	**30**	**25**	**27**	**25**	**27**	**28**	**25.1**
Tiempo Máximo (ms)	**148**	**160**	**185**	**134**	**222**	**171**	**176**	**132**	**161**	**235**	**172.4**
Tiempo Promedio (ms)	**73**	**60**	**70**	**70**	**82**	**80**	**79**	**58**	**62**	**82**	**71.6**

Tabla 4.7.9 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**512**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	**37**	**24**	**34**	**22**	**24**	**35**	**23**	**32**	**21**	**24**	**27.6**
Tiempo Máximo (ms)	**284**	**213**	**174**	**133**	**125**	**122**	**188**	**179**	**158**	**201**	**177.7**
Tiempo Promedio (ms)	**112**	**63**	**80**	**53**	**52**	**66**	**81**	**75**	**78**	**89**	**74.9**

Tabla 4.7.10 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**1518**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	**40**	**38**	**29**	**25**	**44**	**37**	**24**	**39**	**35**	**34**	**34.5**
Tiempo Máximo (ms)	**390**	**230**	**171**	**126**	**220**	**173**	**118**	**153**	**142**	**175**	**189.5**
Tiempo Promedio (ms)	**122**	**79**	**82**	**60**	**99**	**93**	**77**	**71**	**84**	**78**	**84.5**

Tabla 4.7.11 Datos obtenidos para una trama de 1518 bytes.

LATENCIA			
Tamaño de Trama (bytes)	**64**	**512**	**1518**
Tiempo Mínimo (ms)	**25.1**	**27.6**	**34.5**
Tiempo Máximo (ms)	**172.4**	**177.7**	**189.5**
Tiempo Promedio (ms)	**71.6**	**74.9**	**84.5**

Tabla 4.7.12 Comparación de datos obtenidos de las diferentes tramas.

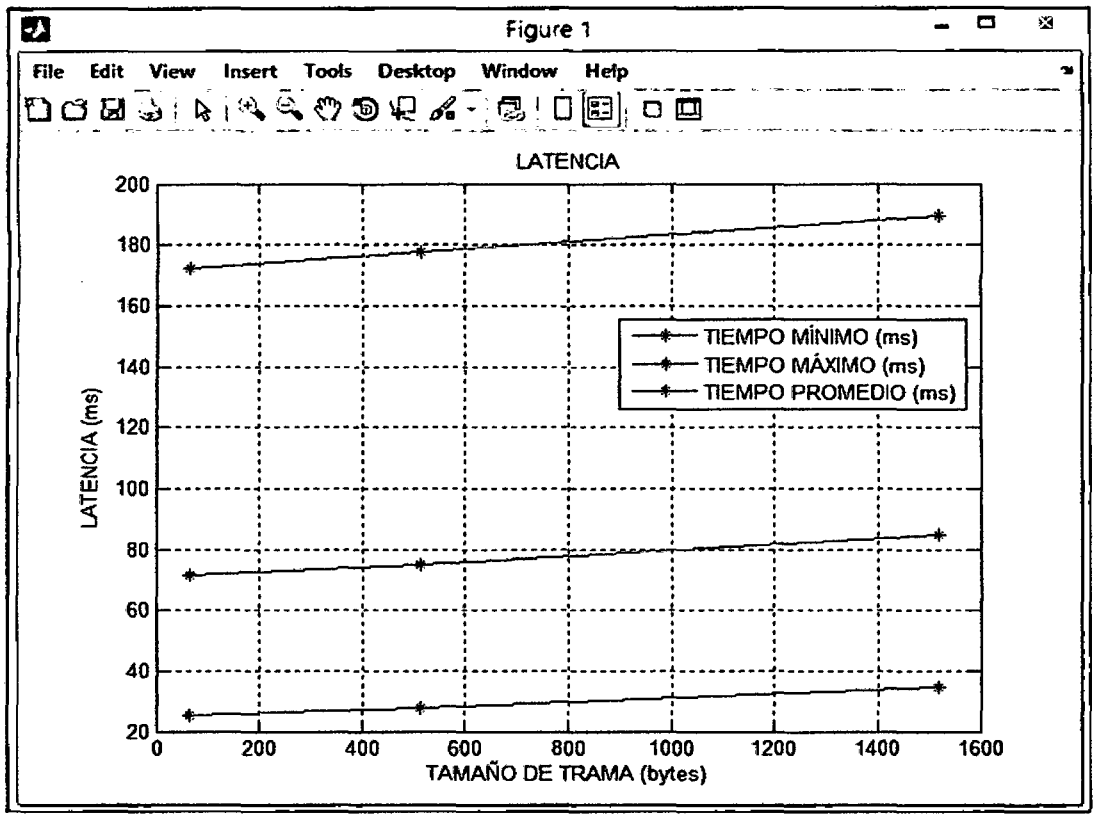


Fig. 4.7.15 Datos representados gráficamente de la variación de la latencia.

De acuerdo con los datos obtenidos, se puede observar claramente que los valores mínimo (color azul), máximo (color rojo) y promedio (color verde) de la latencia de la red se incrementan conforme se envía una trama de longitud mayor, en este caso con la trama de 1518 bytes se obtiene una latencia promedio de 84.5 ms a diferencia de una trama de 64 bytes con 71.6 ms.

PASO 2: Medición del Throughput

Para la medición del Throughput y Jitter se envió una cantidad de tramas a velocidades diferentes durante 20 segundos, hasta encontrar la máxima cantidad de tramas recibidas sin que se produzcan perdidas de las mismas en el router y PC REAL. Como se utilizó Jperf el cliente será el encargado de enviar los paquetes y el servidor los recibirá, indicando la cantidad de paquetes que llegaron correctamente considerando un tamaño del paquete UDP de 750, 1125, 1500 y 1470 (default) bytes, tal como se especifica en el RFC 768.

Configuración del Jperf como servidor para medir Throughput:

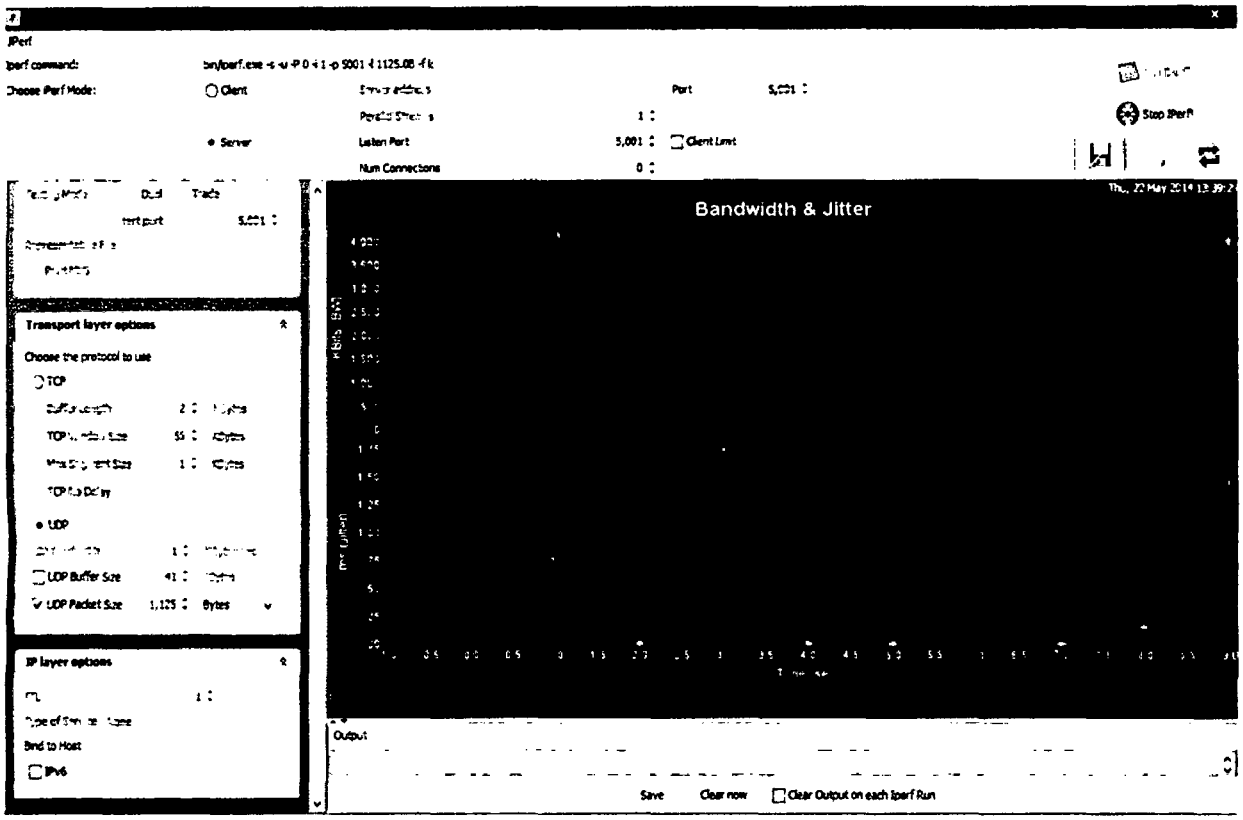


Fig. 4.7.16 Gráfico del Bandwidth y Jitter en Jperf.

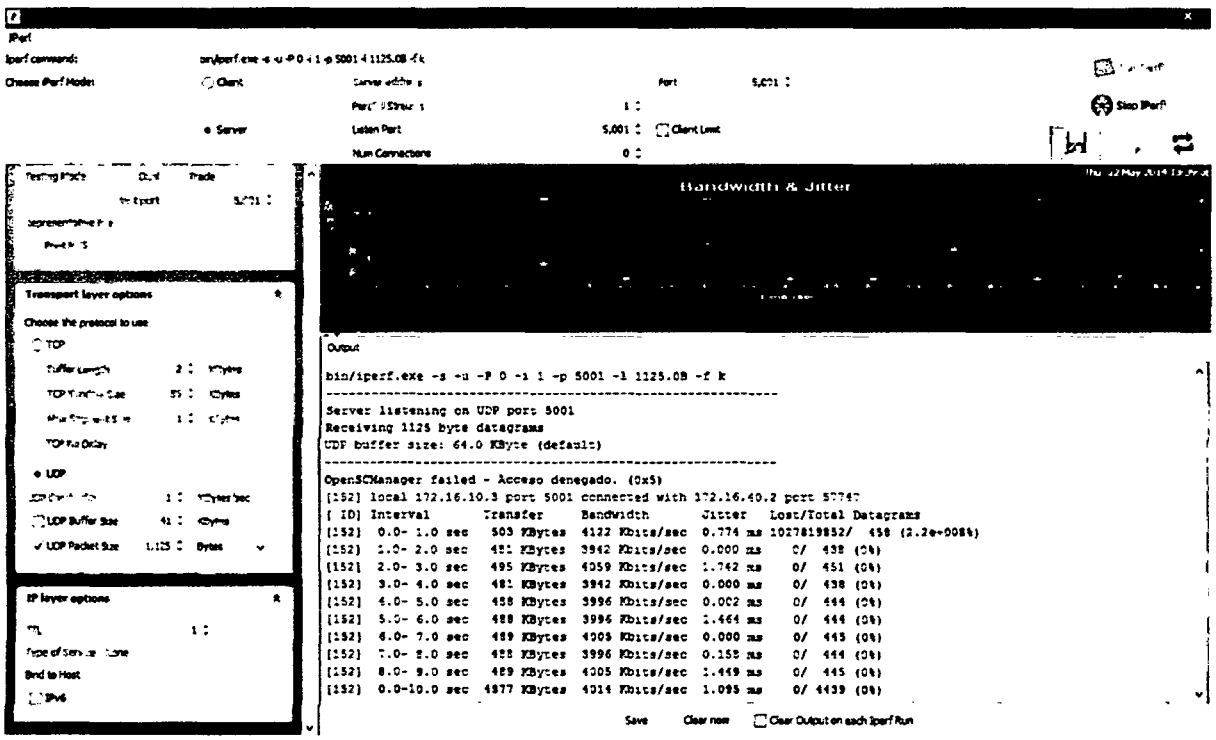


Fig. 4.7.17 Configuración del Jperf como Servidor para medir Jitter.

Configuración del Jperf como cliente para medir Throughput:

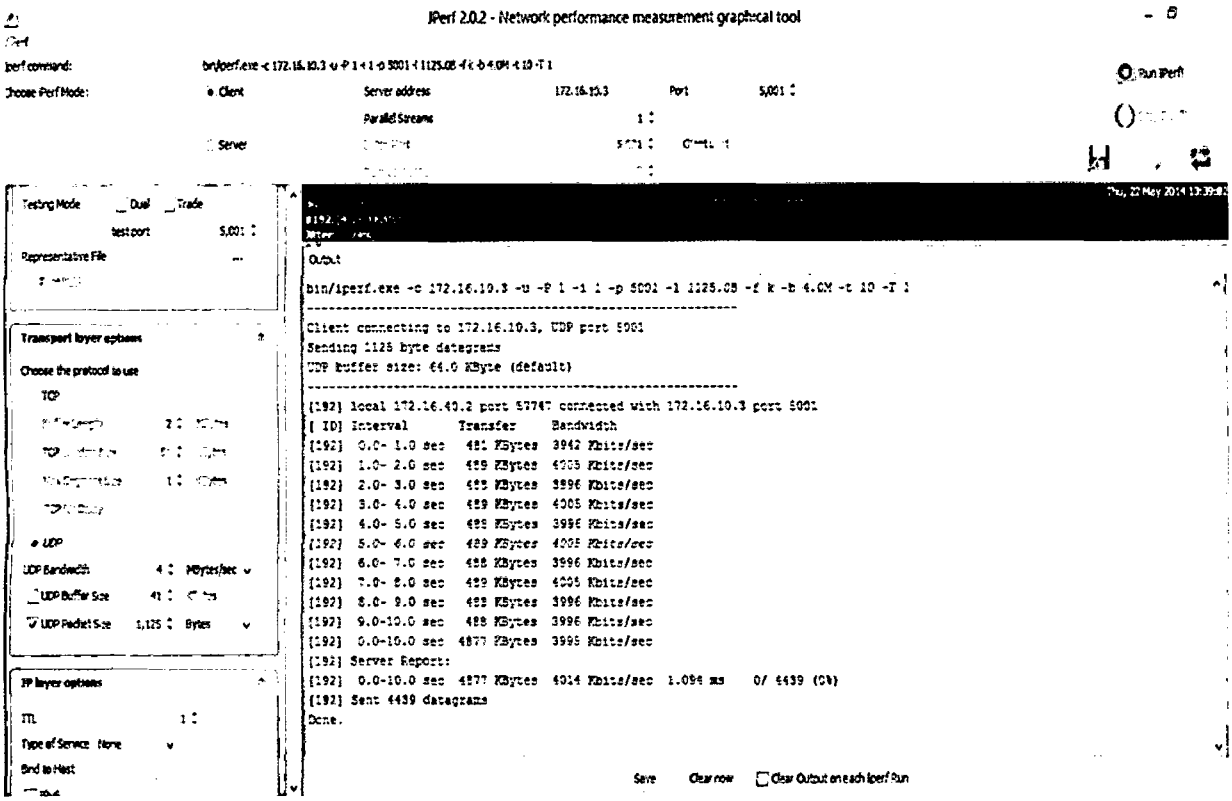


Fig. 4.7.18 Configuración del Jperf como Cliente para medir Throughput.

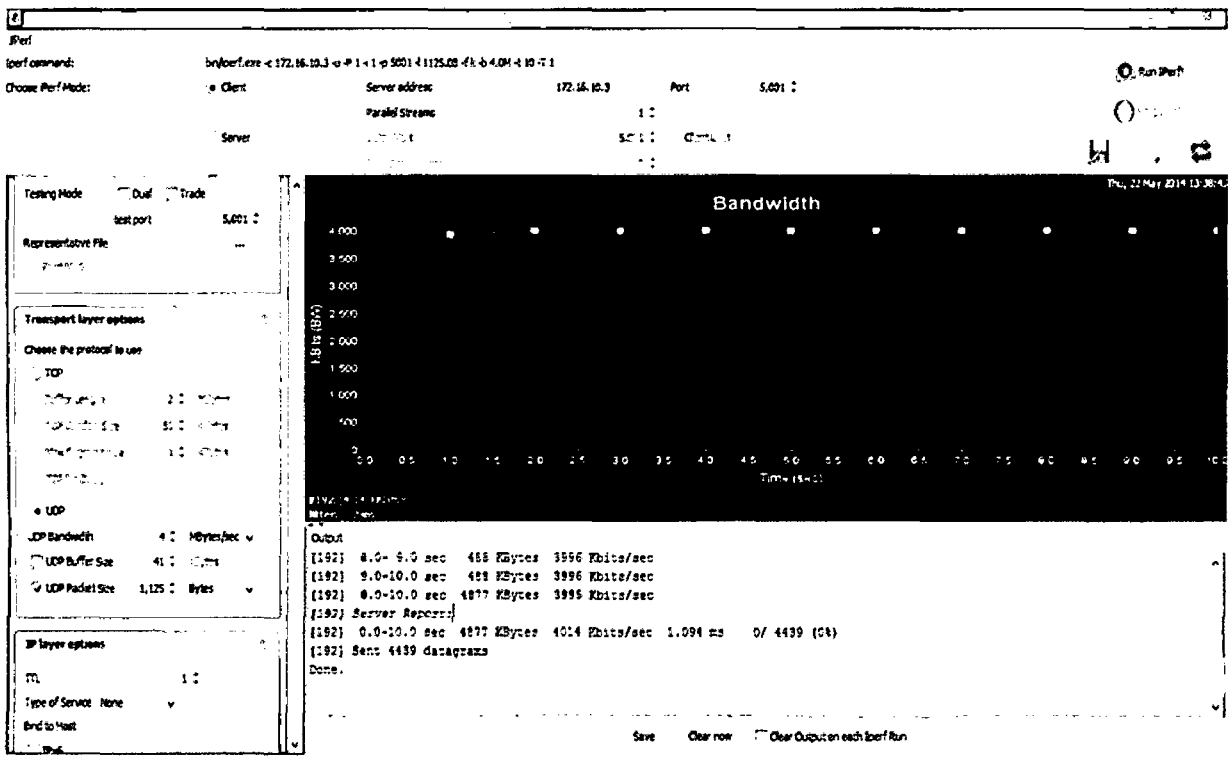


Fig. 4.7.19 Gráfico del Bandwidth en Jperf.

En las siguientes Tablas se detalla los valores del Throughput obtenidos una vez realizada todas las muestras.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**4**	**4**	**4**
Velocidad de Rx (Mbps)	**4**	**4**	**4**
Tramas Transmitidas	**6659**	**4439**	**3335**
Tramas Recibidas	**6659**	**4439**	**3335**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**666**	**444**	**333**

Tabla 4.7.13 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**2**	**5**	**8**
Velocidad de Rx (Mbps)	**2**	**5**	**8**
Tramas Transmitidas	**1701**	**4249**	**6798**
Tramas Recibidas	**1701**	**4249**	**6798**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**170**	**425**	**680**

Tabla 4.7.14 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

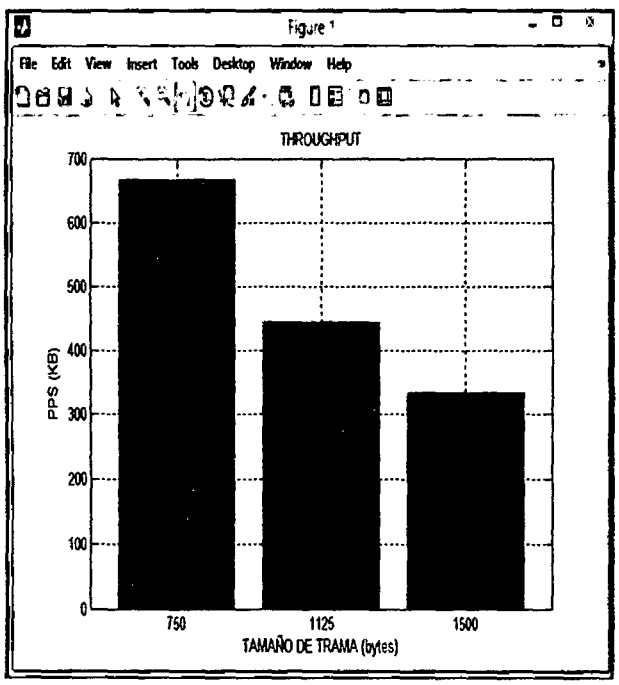


Fig. 4.7.20 PPS vs. Tamaño de Trama

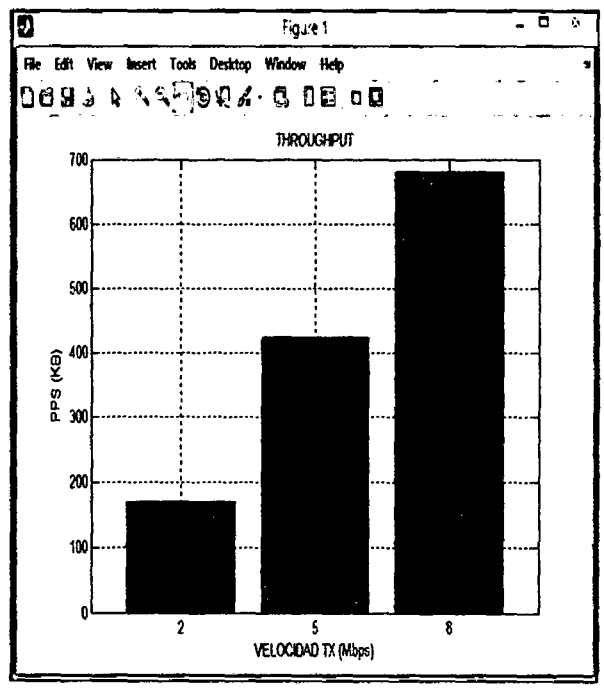


Fig. 4.7.21 PPS vs. Velocidad Tx

En la figura 4.7.20, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 750 bytes, 1125 bytes y 1500 bytes los cuales han utilizado una velocidad de Tx constante de 4 Mbps, en la gráfica se puede observar claramente que al enviar una trama de 750 bytes se envía 666 pps, con una trama de 1125 se envía 444 pps y con una trama de 1500 se envía 333 pps.

Mientras en la figura 4.7.21, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 1470 bytes los cuales han utilizado una velocidad de Tx variada desde 2 Mbps hasta 8 Mbps sin que se produzcan perdidas en el envío, en la gráfica se observa que a 2 Mbps se envían 170 pps, en cambio a 8 Mbps se obtiene 680 pps.

PASO 3: Medición del Jitter

Para la medición se envió datos UDP de longitud variable a velocidades diferentes de Throughput obtenida anteriormente durante 20 segundos. Como se utilizó anteriormente Jperf el cliente será el encargado de enviar los datos y el servidor los recibirá, indicando los valores de Jitter obtenidos durante la transmisión de los datos.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (kbps)	**4**	**4**	**4**
Velocidad de Rx (kbps)	**4**	**4**	**4**
Tramas Transmitidas	**6659**	**4439**	**3335**
Tramas Recibidas	**6659**	**4439**	**333**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**0.01**	**1.095**	**1.288**

Tabla 4.7.15 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (kbps)	**2**	**5**	**8**
Velocidad de Rx (kbps)	**2**	**5**	**8**
Tramas Transmitidas	**1701**	**4249**	**6798**
Tramas Recibidas	**1701**	**4249**	**6798**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**0.950**	**0.02**	**0.014**

Tabla 4.7.16 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

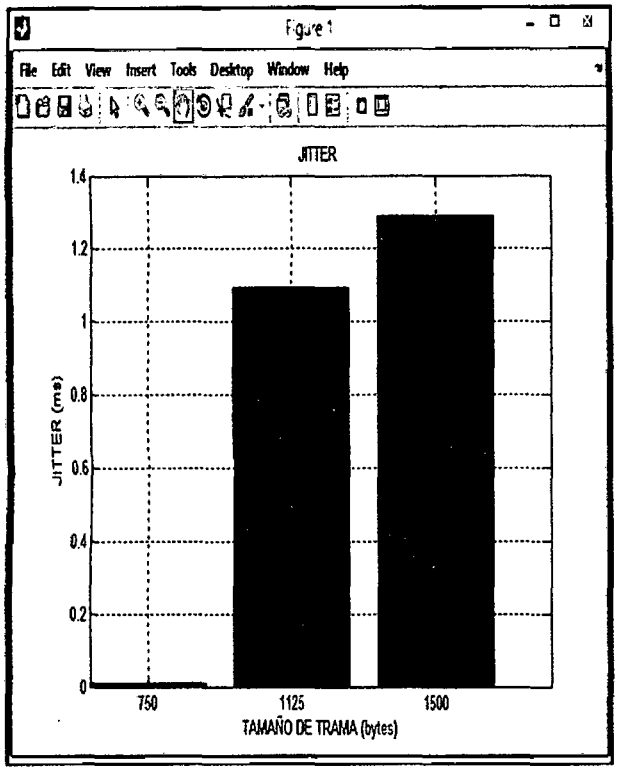


Fig. 4.7.22 Jitter vs. Tamaño de Trama

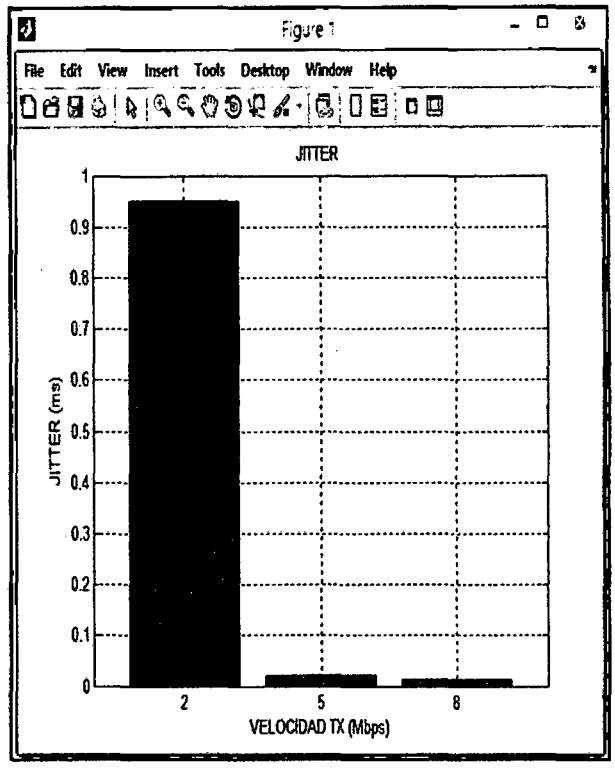


Fig. 4.7.23 Jitter vs. Velocidad Tx

En la figura 4.7.22 se observa los valores del Jitter obtenidos al enviar diferentes tamaños de paquete UDP como 750, 1125 y 1500 bytes utilizando una velocidad de Tx constante de 4 Mbps, se puede observar claramente que con una trama de 750 bytes se tiene un Jitter de 0.01 ms a diferencia de la trama de 1500 bytes en la cual se tiene un Jitter de 1.288 ms.

En la figura 4.7.23, se observa los valores del Jitter obtenidos al enviar paquetes UDP de 1470 bytes utilizando una velocidad de Tx que varía entre los 2 Mbps y los 8 Mbps, se puede observar claramente que con una velocidad Tx de 2 Mbps se tiene un Jitter de 0.950 ms a diferencia que a una velocidad Tx de 8 Mbps en la cual se tiene un Jitter de 0.014 ms.

Medición de Jitter a 8 Mbps:

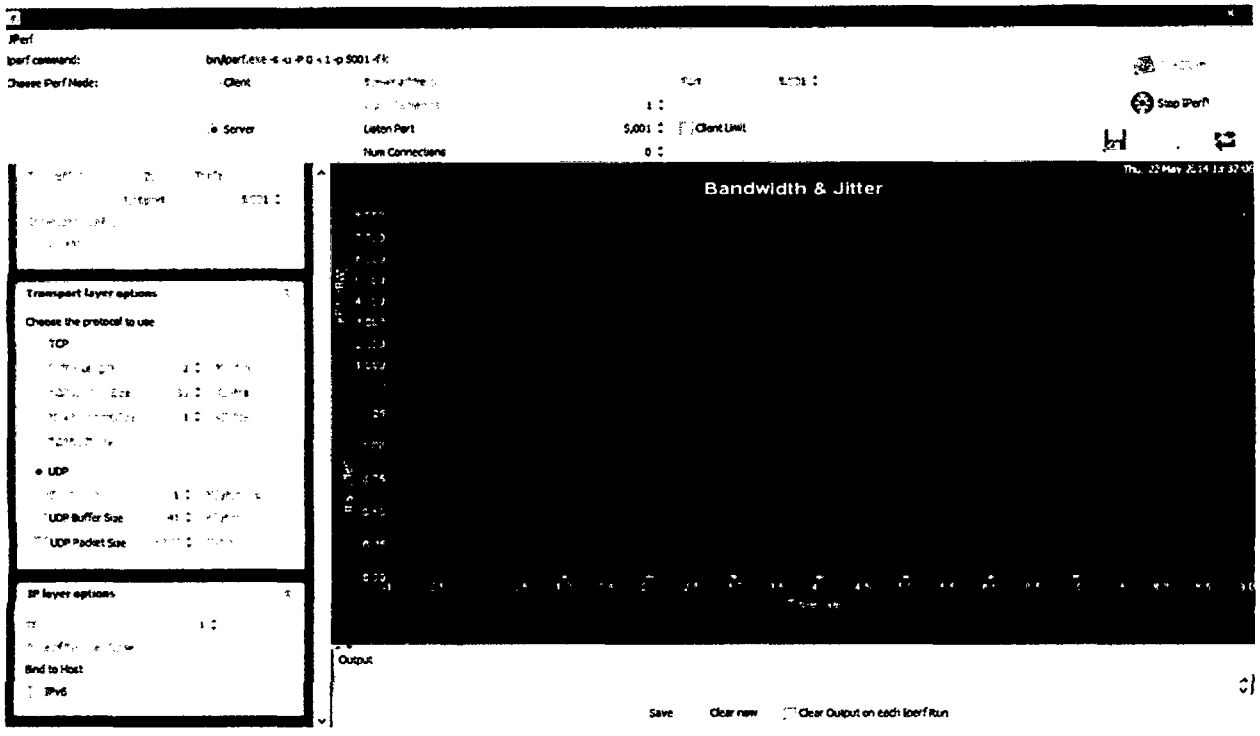


Fig. 4.7.24 Gráfica de Bandwidth y Jitter.

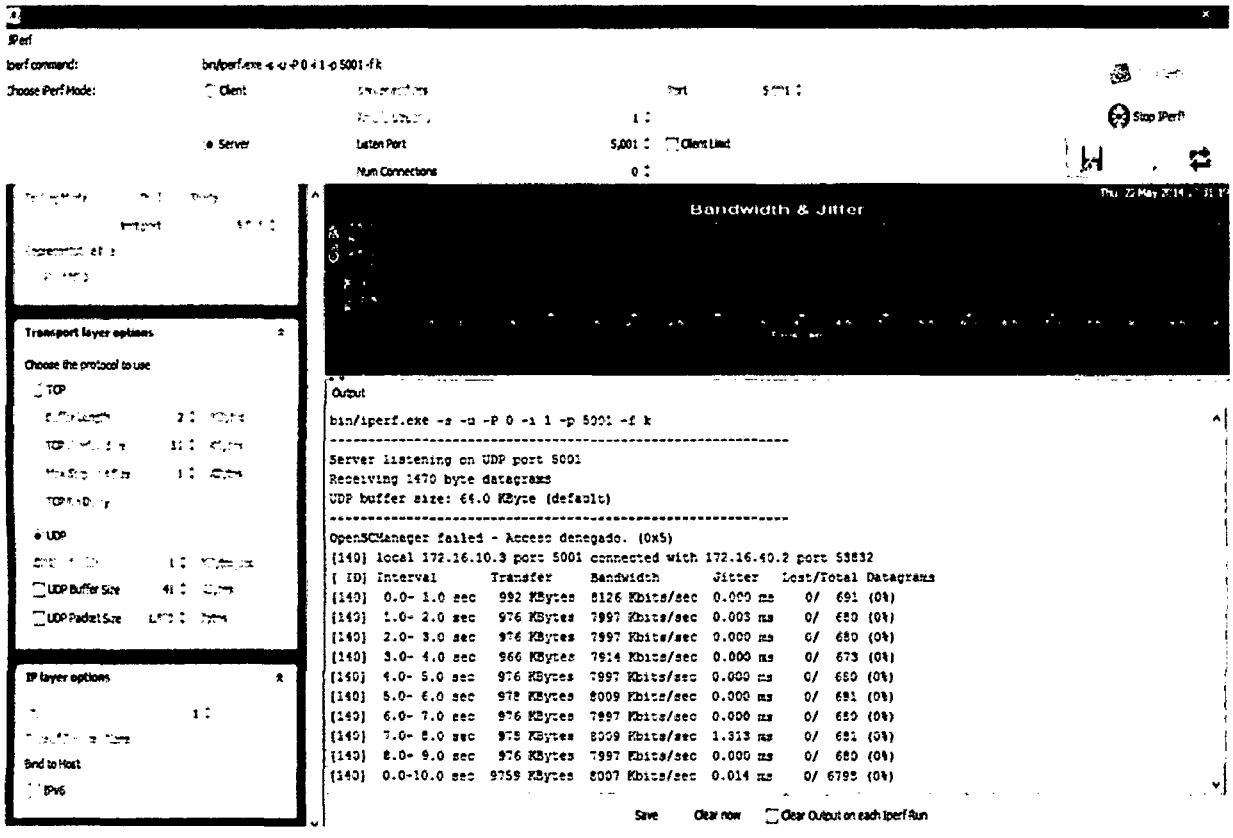


Fig. 4.7.25 Resultados al medir Throughput como servidor.

PASO 4: Captura de tráfico con Wireshark.

Capturar tráfico de paquetes en la interfaz f1/0 de R1.

- Captura de paquetes ICMP.

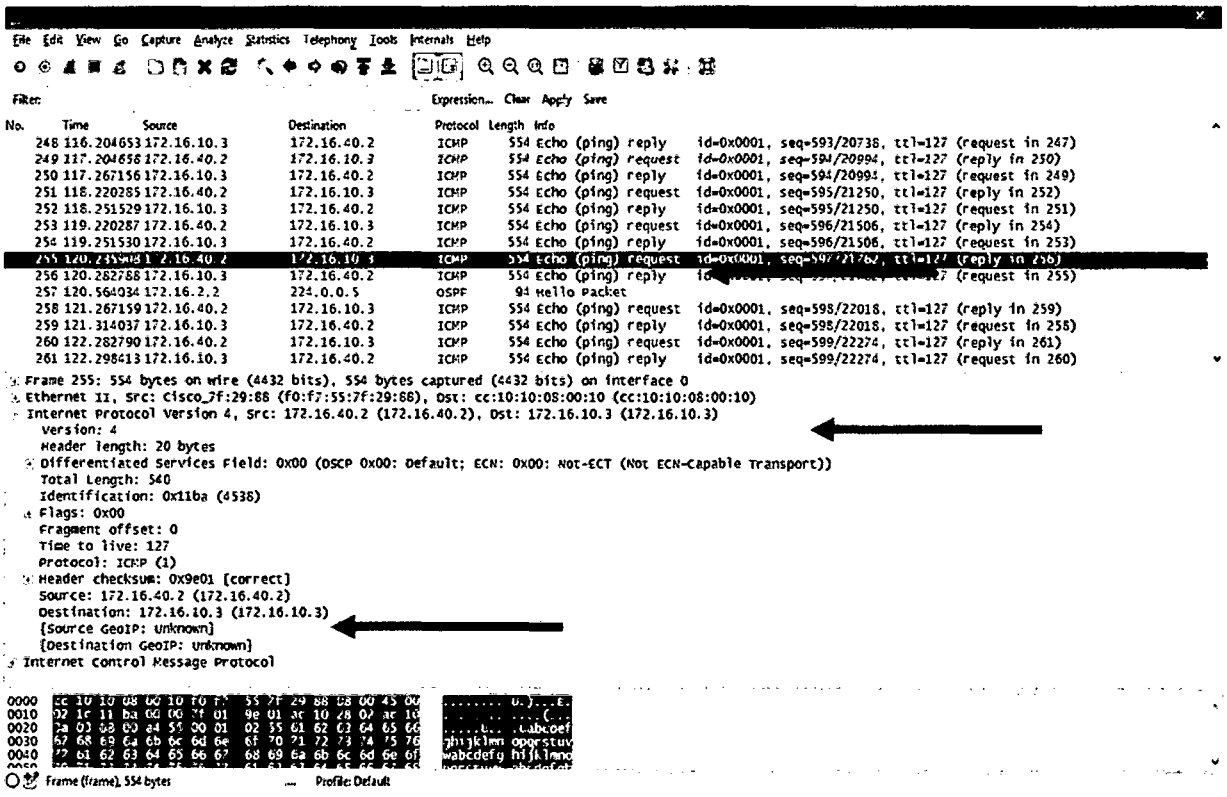


Fig. 4.7.26 Captura de tráfico en la red con Wireshark.

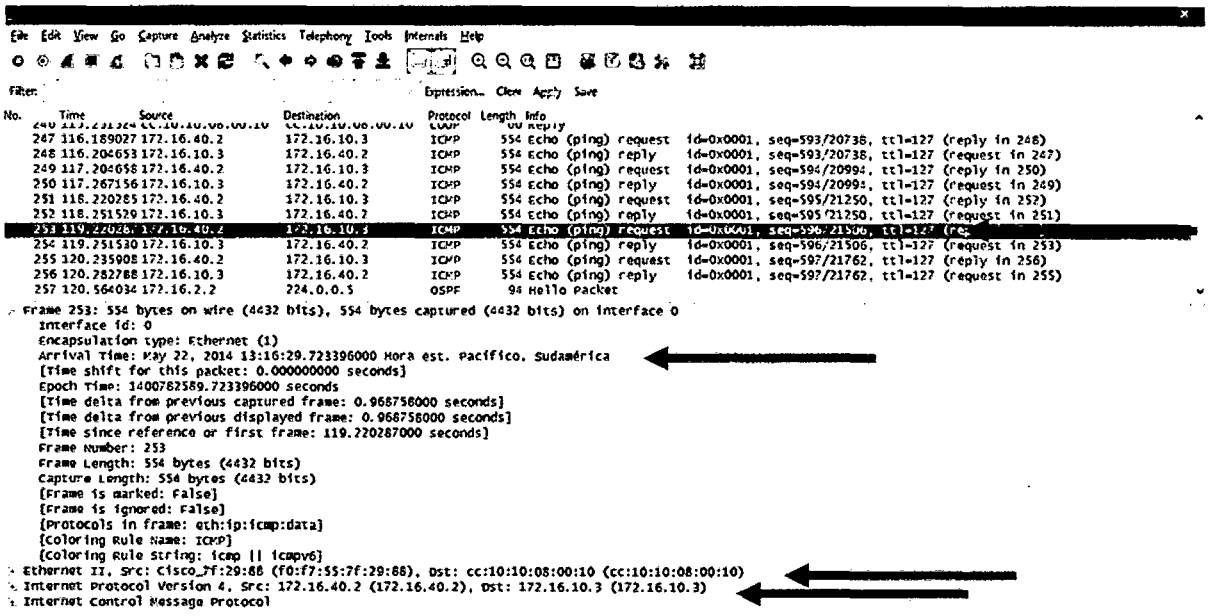


Fig. 4.7.27 Información detallada del paquete ICMP.

- Protocolo de enrutamiento OSPF:

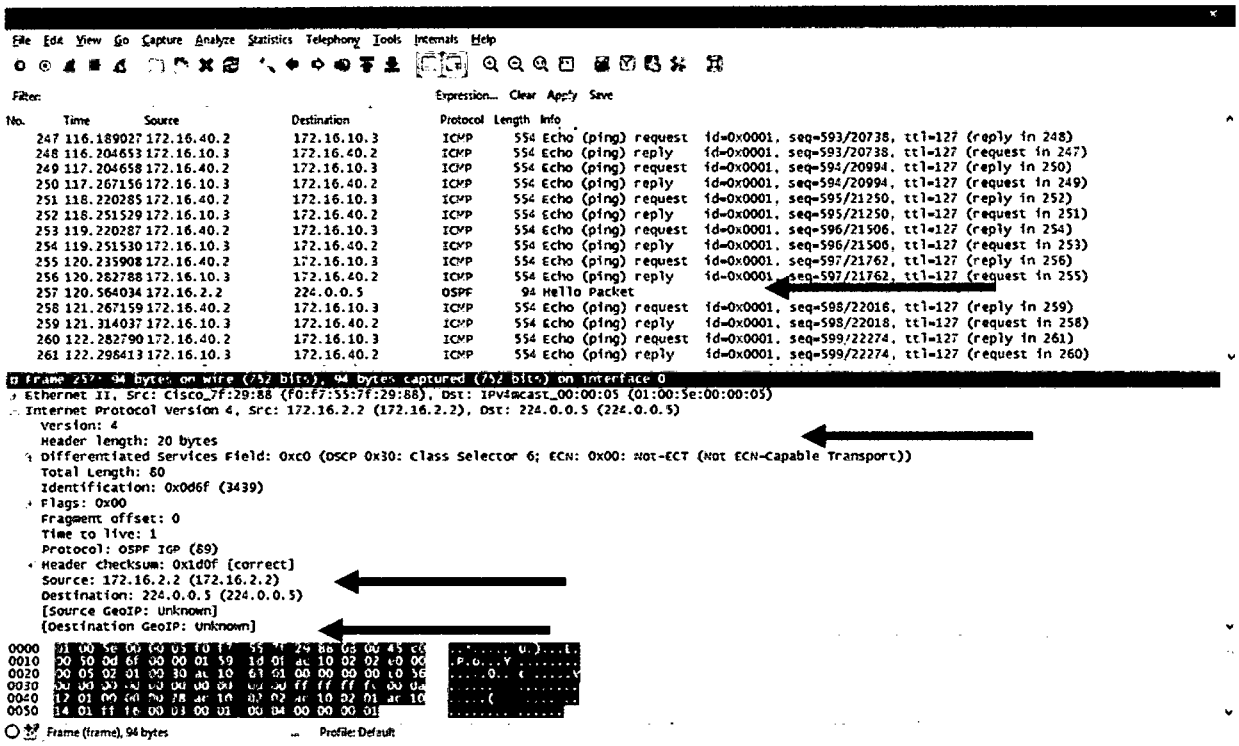


Fig. 4.7.28 Captura del protocolo OSPF con Wireshark.

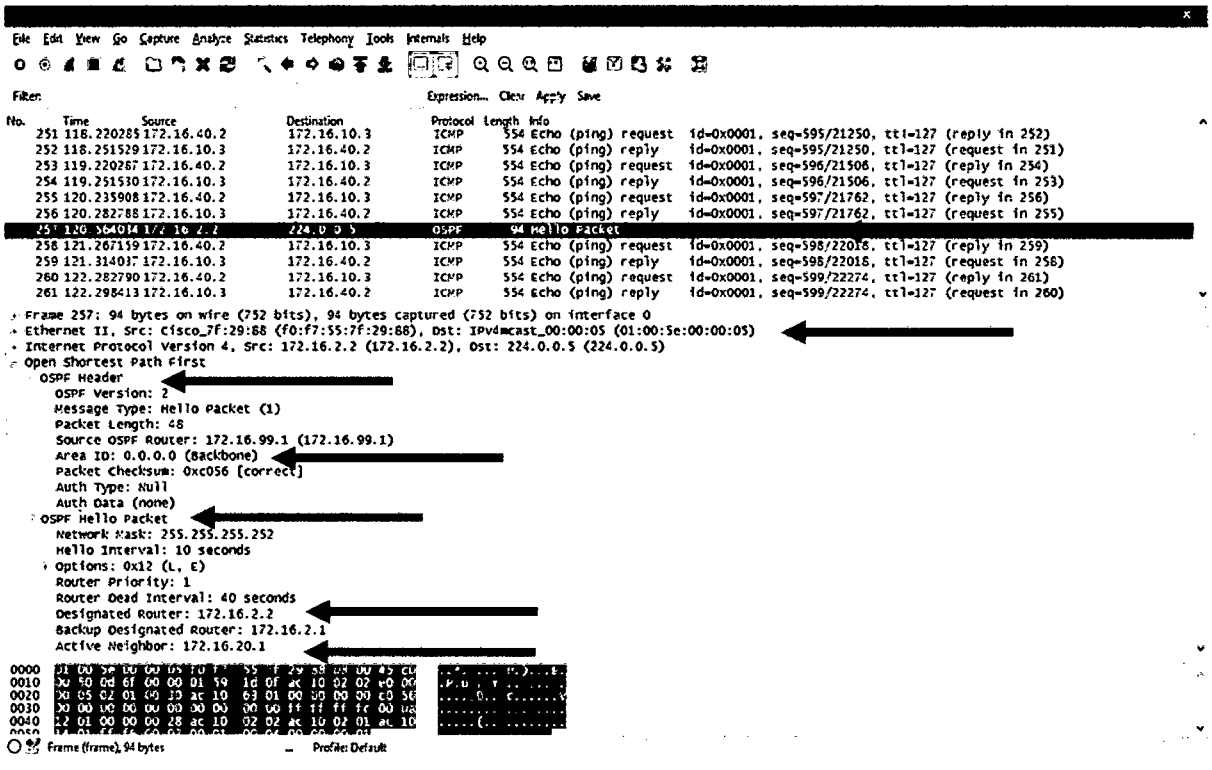


Fig. 4.7.29 Información detallada del protocolo OSPF.

LABORATORIO 4.8: CONFIGURACION BÁSICA DE ETHERCHANNEL

REVISIÓN TEÓRICA:

OBJETIVOS DE APRENDIZAJE

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología.
- Borrar las configuraciones y volver a cargar un switch y un router al estado predeterminado.
- Realizar las tareas básicas de configuración en una LAN conmutada y un router.
- Configurar las VLAN y el protocolo PORTCHANNEL en todos los switches.
- Configurar un router para admitir el enlace 802.1q en una interfaz Fast Ethernet.
- Configurar un router con subinterfaces que correspondan a las VLAN configuradas.
- Demostrar y explicar el enrutamiento entre VLAN.

ESCENARIO:

En esta actividad de laboratorio, el usuario examinará y configurará switches con sus respectivas VLAN con sus LAN independientes. Esta práctica de laboratorio se armará y conectará la red que se muestra en el Diagrama de topología teniendo en cuenta los siguientes requisitos:

Vlan 10: 180 host.

Vlan 20: 150 host.

Vlan 30: 200 host.

Vlan 40: 220 host.

Luego realice las configuraciones básicas en los routers y switch, para que se realice la comunicación entre los hosts de las vlan. Después de completar la configuración pruebe la conectividad entre los dispositivos de la red y finalmente analizará el tráfico de paquetes en dicha topología.

DIAGRAMA DE TOPOLOGÍA:

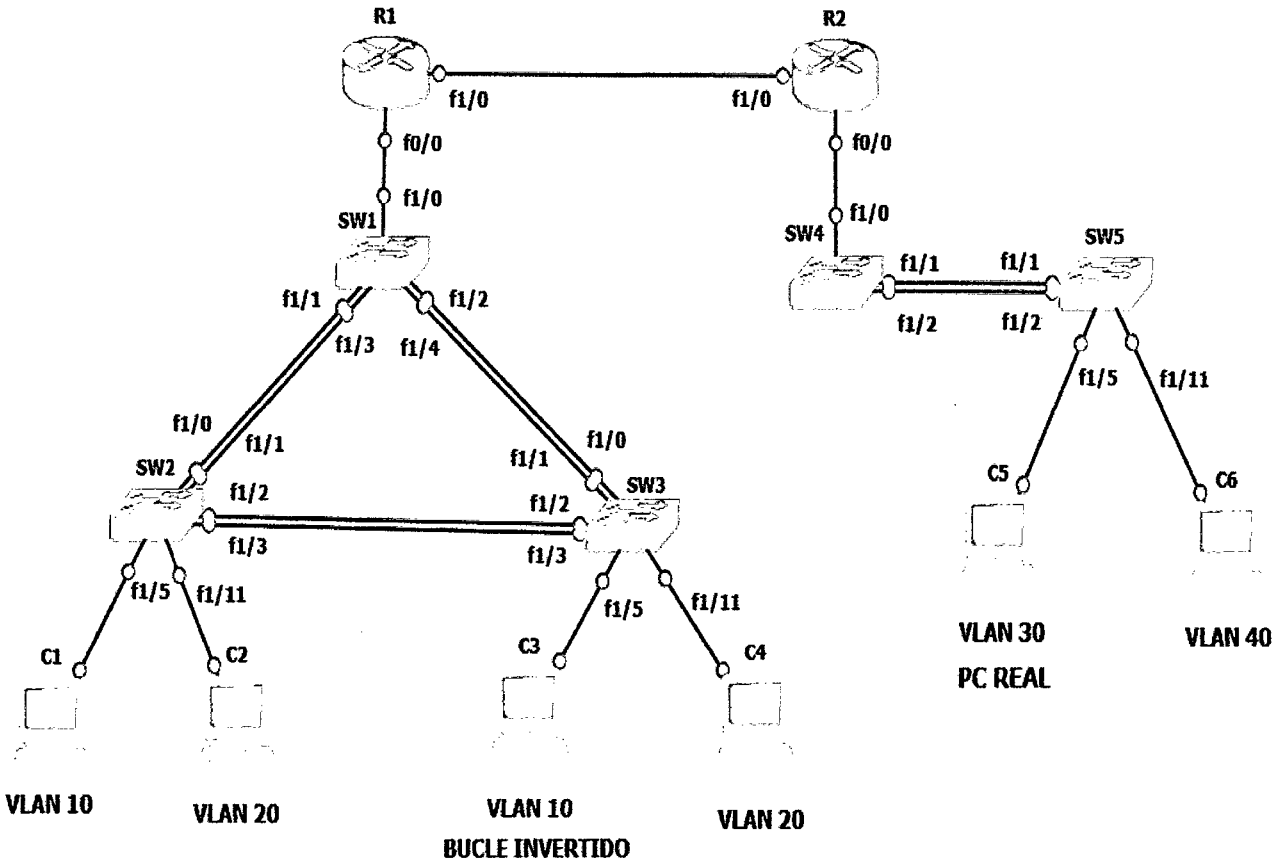


Fig. 4.8.1 Red Virtual en GNS3.

TAREA 1: MONTAR LA RED EN GNS3

PASO 1: Montar y conectar la red igual a la del Diagrama de topología.

PASO 2: Borrar toda configuración existente en los switches.

En los switches borre la NVRAM, borre el archivo vlan.dat y reinicie los switches (solo en los switch físicos). Después de que la recarga se haya completado, utilice el comando **show vlan-sw** para verificar que solo existan VLAN predeterminadas y que todos los puertos se asignen a la VLAN 1, este comando solo es para GNS3 para los switch físicos solo es el comando **show vlan**.

PASO 3: Borrar la configuración en el router y volver a cargar.

Router#**erase startup-config**

Erasing the nvram filesystem will remove all configuration files! Continue?

[confirm]

Erase of nvram: complete

Router#**reload**

System configuration has been modified. Save? [yes/no]: **no**

TAREA 2: REALICE EL DIRECCIONAMIENTO IP PARA LAS REDES LAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	f1/0	172.17.2.1	255.255.255.252	No aplicable
	f0/0.1	172.17.1.1	255.255.255.0	No aplicable
	f0/0.10	172.17.10.1	255.255.255.0	No aplicable
	f0/0.20	172.17.20.1	255.255.255.0	No aplicable
R2	f1/0	172.17.2.2	255.255.255.0	No aplicable
	f0/0.30	172.17.30.1	255.255.255.0	No aplicable
	f0/0.40	172.17.40.1	255.255.255.0	No aplicable
	f0/0.1	172.17.99.1	255.255.255.0	No aplicable
C3	BUCLE INVERTIDO	172.17.10.2	255.255.255.0	172.16.10.1
C1	VPCS	172.17.10.3	255.255.255.0	172.16.10.1
C2	VPCS	172.17.20.2	255.255.255.0	172.16.20.1
C4	VPCS	172.17.20.3	255.255.255.0	172.16.20.1
PC VLAN 30	NIC	172.17.30.2	255.255.255.0	172.16.30.1
C6	VPCS	172.17.40.2	255.255.255.0	172.16.40.1

Tabla 4.8.1 Direccionamiento IP para las Redes.

ASIGNACIONES DE PUERTO: SW1

Puertos	Asignación	Red
f 1/0 – f 1/4	Enlaces troncales 802.1q (LAN 1 nativa)	**172.17.1.0 /24**

Tabla 4.8.2 Asignación de Puertos SW1.

ASIGNACIONES DE PUERTO: SW2

Puertos	Asignación	Red
f1/0 – f1/3	Enlaces troncales 802.1q (LAN 1 nativa)	**172.17.1.0 /24**
f1/5 – f1/9	Vlan 10	**172.17.10.0 /24**
f1/10 – f1/15	Vlan 20	**172.17.20.0 /24**

Tabla 4.8.3 Asignación de Puertos SW2.

ASIGNACIONES DE PUERTO: SW3

Puertos	Asignación	Red
f1/0 – f1/3	Enlaces troncales 802.1q (LAN 1 nativa)	**172.17.1.0 /24**
f1/5 – f1/9	Vlan 10	**172.17.10.0 /24**
f1/10 – f1/15	Vlan 20	**172.17.20.0 /24**

Tabla 4.8.4 Asignación de Puertos SW3.

ASIGNACIONES DE PUERTO: SW4

Puertos	Asignación	Red
f1/0 – f1/2	Enlaces troncales 802.1q (LAN 99 nativa)	**172.17.99.0 /24**

Tabla 4.8.5 Asignación de Puertos SW4.

ASIGNACIONES DE PUERTO: SW5

Puertos	Asignación	Red
f1/0 – f1/1	Enlaces troncales 802.1q (LAN 99 nativa)	**172.17.99.0 /24**
f1/1 – f1/10	Vlan 30	**172.17.30.0 /24**
f1/11 – f1/20	Vlan 40	**172.17.40.0/24**

Tabla 4.8.6 Asignación de Puertos SW5.

TAREA 3: REALIZAR LA CONFIGURACION BASICA DEL ROUTER Y SWITCHES

Una vez iniciado el equipo aparecerá el siguiente prompt:

Router>

Ingrese al modo privilegiado

Router>enable

Aparece el siguiente prompt

Router#

Switch>

Ingrese al modo privilegiado

Switch >enable

Aparece el siguiente prompt

Switch #

PASO 1: Establezca la configuración global del nombre de host.

En el modo exec privilegiado, ingrese al modo de configuración global:

Router# **configure terminal**

Switch # **configure terminal**

Ingrese el siguiente comando para configurar el nombre del router:

Router(config)#**hostname XXXXXX** (Escribir nombre deseado)

Switch(config)#**hostname XXXXXX**

PASO 2: Configure un mensaje para que se muestre al ingresar al router.

Router(config)#**banner motd %** Solo acceso a personal autorizado **%** (Puede escribir cualquier mensaje)

El símbolo % indica el inicio y final del mensaje

Switch(config)# **banner motd %** Solo acceso a personal autorizado **%**

PASO 3: Configure las contraseñas de consola, enable secret y VTY.

Seguir los siguientes pasos para el switches:

Switch(config)# **line console 0**

Switch(config-line)# **password XXXXX**

Switch(config-line)# **login**

Switch(config-line)# **exit**

Switch(config)# **enable secret XXXXX**

Switch(config)# **line vty 0 4**

Switch(config-line)# **password XXXXX**

Switch(config-line)# **login**

Switch(config-line)# **exit**

PASO 4: Desactive la búsqueda DNS.

Router(config)# **no ip-domain lookup**

Si escribes algo que no sea un comando de Cisco IOS o cometes un error, el router asume que ha escrito un nombre de dominio y trata de resolver lo que usted escribe, realizando una búsqueda de DNS.

PASO 5: Sincronice los mensajes no solicitados y el resultado de la depuración con el resultado solicitado y los indicadores para las líneas de consola y de terminal virtual.

Router(config)# **line console 0**

Router(config)# **logging synchronous**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **logging synchronous**

Router(config)# **exit**

PASO 6: Configure un tiempo de espera EXEC de 10 minutos.

Router(config)# **line console 0**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

PASO 7: Guardar la configuración.

Router(config)# **copy running-config startup-config**

NOTA: Realizar la misma programación para los router's.

TAREA 4: CONFIGURE Y ACTIVE LAS INTERFACES FASTETHERNET.

Aplique Los siguientes comandos:

R1:

Configuración para una interface fasEthernet:

R1(config)# **interface fasEthernet 1/0**

R1(config-if)# **description conexion a R2**

R1(config-if)# **ip address 172.17.2.1 255.255.255.252**

R1(config-if)# **no shutdown**

R1(config-if)# **end**

R2:

Configuración para una interface fastEthernet:

R2(config)# **interface fastEthernet 0/0**

R2(config-if)# **description conexion a R1**

R2(config-if)# **ip address 172.17.2.2 255.255.255.252**

R2(config-if)# **no shutdown**

R2(config-if)# **end**

TAREA 5: CONFIGURAR VTP EN LOS SWITCHES

PASO 1: Configurar VTP en los cinco switches, recuerde que las contraseñas y los nombres de dominios VTP distinguen entre mayúsculas y minúsculas.

SW4:

SW4(config)#**vtp mode server**

SW4(config)#**vtp domain unprg**

SW4(config)#**vtp password unprg**

SW5:

SW5(config)#**vtp mode client**

SW5(config)#**vtp domain unprg**

SW5(config)#**vtp password unprg**

SW1:

SW1# **vlan database**

SW1(vlan)# **vtp server**

SW1(vlan)# **vtp domain unprg**

SW1(vlan)# **vtp password unprg**

SW2:

SW2# **vlan database**

SW2(vlan)# **vtp client**

SW2(vlan)# **vtp domain unprg**

SW2(vlan)# **vtp password unprg**

SW3:

SW3# **vlan database**

SW3(vlan)# **vtp client**

SW3(vlan)# **vtp domain unprg**

SW3(vlan)# **vtp password unprg**

TAREA 6: CONFIGURAR LAS VLAN EN EL SERVIDOR VTP.

PASO 1: Configure las siguientes VLAN en los servidores VTP:

SW1:

Vlan	Nombre de la Vlan
Vlan 10	Vlan-electronica
Vlan 20	Vlan-mecanica

Tabla 4.8.7 Nombre de VLAN en SW1.

SWA:

Vlan	Nombre de la Vlan
Vlan 99	Vlan-administracion
Vlan 30	Vlan-matematica
Vlan 40	Vlan-fisica

Tabla 4.8.8 Nombre de VLAN en SW4.

SW4:

SW4(config)#**vlan 99**

SW4(config-vlan)#**name vlan-administracion**

SW4(config-vlan)#**exit**

SW4(config)#**vlan 30**

SW4(config-vlan)#**name vlan-matematica**

SW4(config-vlan)#**exit**

SW4(config)#**vlan 40**

SW4(config-vlan)#**name vlan-fisica**

SW4(config-vlan)#**exit**

SW1:

SW1# **vlan database**

SW1(vlan)# **vlan 10 name vlan-electronica**

SW1(vlan)# **vlan 20 name vlan-mecanica**

SW1(vlan)#**exit**

PASO 2: Configuración de puertos de los enlace troncales con etherhannel.

SW4:

SW4(config)# **interface fasEthernet 0/0**

SW4(config-if)#**switchport mode trunk**

SW4(config-if)#**no shutdown**

SW4(config-if)# **exit**

SW4(config)#**interface range fa0/1 – 2**

SW4(config-if-range)#**channel-group 1 mode on**

SW4(config-if-range)#**switchport mode trunk**

SW4(config-if-range)#**no shutdown**

SW4(config-if-range)#**end**

SW5:

SW5(config)# **interface range fa0/1 - 2**

SW5(config-if-range)#**channel-group 1 mode on**

SW5(config-if-range)#**switchport mode trunk**

SW5(config-if-range)#**no shutdown**

SW5(config-if-range)#**end**

Configure Fa1/0, Fa1/1 y Fa1/2 como puertos de enlace troncales.

SW1:

SW1(config)# **interface fasEthernet 1/0**

SW1(config-if)#**switchport mode trunk**

SW1(config-if)# **exit**

SW1(config)# **interface fasEthernet 1/1**

SW1(config-if-range)#**channel-group 1 mode on**

SW1(config-if-range)#**switchport mode trunk**

SW1(config-if)# **exit**

SW1(config)# **interface fasEthernet 1/3**

SW1(config-if-range)#**channel-group 1 mode on**

SW1(config-if-range)#**switchport mode trunk**

SW1(config-if)# **exit**

SW1(config)# **interface fasEthernet 1/2**

SW1(config-if-range)#**channel-group 2 mode on**

SW1(config-if-range)#**switchport mode trunk**

SW1(config-if)# **exit**

SW1(config)# **interface fasEthernet 1/4**

SW1(config-if-range)#**channel-group 2 mode on**

SW1(config-if-range)#**switchport mode trunk**

SW1(config-if)# **exit**

SW2:

SW2(config)# **interface range fasEthernet 1/0 – 1**

SW2(config-if-range)#**channel-group 1 mode on**

SW2(config-if-range)#**switchport mode trunk**

SW2(config-if)# **exit**

SW2(config)# **interface range fasEthernet 1/2 – 3**

SW2(config-if-range)#**channel-group 2 mode on**

SW2(config-if-range)#**switchport mode trunk**

SW2(config-if)# **exit**

SW3:

SW3(config)# **interface range fasEthernet 1/0 – 1**

SW3(config-if-range)#**channel-group 1 mode on**

SW3(config-if-range)#**switchport mode trunk**

SW3(config-if)# **exit**

SW3(config)# **interface range fasEthernet 1/2 – 3**

SW3(config-if-range)#**channel-group 2 mode on**

SW3(config-if-range)#**switchport mode trunk**

SW3(config-if)# **exit**

PASO 3: Asignar puertos de los switches a las VLAN.

Consulte la tabla de asignación de puertos al principio del laboratorio para asignar puertos a las VLAN.

SW5:

SW5(config)#**interface range fa0/5 - 9**

SW5(config-if-range)#**switchport access vlan 30**

SW5(config-if-range)#**switchport mode access**

SW5(config-if-range)#**interface range fa0/10 - 15**

SW5(config-if-range)#**switchport mode access**

SW5(config-if-range)#**switchport access vlan 40**

SW5(config-if-range)#**end**

SW5#**copy running-config startup-config**

SW2:

SW2(config)#**interface range fa0/5 - 10**

SW2(config-if-range)#**switchport mode access**

SW2(config-if-range)#**switchport access vlan 10**

SW2(config-if-range)#**interface range fa0/11 - 15**

SW2(config-if-range)#**switchport mode access**

SW2(config-if-range)#**switchport access vlan 20**

SW2(config-if-range)#**end**

SW2#**copy running-config startup-config**

SW3:

SW3(config)#**interface range fa0/5 – 10**

SW3(config-if-range)#**switchport mode access**

SW3(config-if-range)#**switchport access vlan 10**

SW3(config-if-range)#**interface range fa0/11 – 15**

SW3(config-if-range)#**switchport mode access**

SW3(config-if-range)#**switchport access vlan 20**

SW3(config-if-range)#**end**

SW3#**copy running-config startup-config**

TAREA 7: CONFIGURAR LA INTERFAZ DE ENLACES TRONCALES EN R1 Y R2.

Los comandos son los siguientes:

R1(config)# **interface fasEthernet 0/0.10**

R1(config-subif)# **encapsulation dot1Q 10**

R1(config-subif)# **ip address 172.17.10.1 255.255.255.0**

R1(config-subif)# **exit**

R1(config)#**interface fasEthernet 0/0.20**

R1(config-subif)# **encapsulation dot1Q 20**

R1(config-subif)# **ip address 172.17.20.1 255.255.255.0**

R1(config-subif)# **exit**

R1(config)# **interface fasEthernet 0/0**

R1(config-if)# **no shutdown**

R1(config-if)# **end**

R2(config)# **interface fastEthernet 0/1.30**

R2(config-subif)# **encapsulation dot1Q 30**

R2(config-subif)# **ip address 172.17.30.1 255.255.255.0**

R2(config-subif)# **exit**

R2(config)# **interface fastEthernet 0/1.40**

R2(config-subif)# **encapsulation dot1Q 40**

R2(config-subif)# **ip address 172.17.40.1 255.255.255.0**

R2(config-subif)# **exit**

R2(config)# **interface gigabitEthernet 0/1**

R2(config-if)# **no shutdown**

R2(config-if)# **end**

TAREA 8: CONFIGURE EL PROTOCOLO EIGRP EN EL ROUTER R1 Y R2

R1(config)#**router eigrp 1**
R1(config-router)#**network 172.17.2.0 0.0.0.3**
R1(config-router)#**network 172.17.10.0 0.0.0.255**
R1(config-router)#**network 172.17.20.0 0.0.0.255**
R1(config-router)#**no auto-summary**
R1(config-router)#**end**
R1#**copy run start**
R2(config)#**router eigrp 1**
R2(config-router)#**network 172.17.2.0 0.0.0.3**
R2(config-router)#**network 172.17.30.0 0.0.0.255**
R2(config-router)#**network 172.17.40.0 0.0.0.255**

R2(config-router)#**no auto-summary**
R2(config-router)#**end**
R2#**copy run start**

TAREA 9: CONFIGURE DHCP EN LOS ROUTERS R1 Y R2.

R1:

R1(config)#**ip dhcp pool VLAN-ELECTRONICA**
R1(dhcp-config)#**network 172.17.20.0 255.255.255.0**
R1(dhcp-config)#**default-router 172.17.10.1**
R1(dhcp-config)#**dns-server 200.48.225.130**
R1(dhcp- config)#**exit**
R1(config)#**ip dhcp excluded-address 172.16.20.1**

R1(config)#**ip dhcp pool VLAN-MECANICA**
R1(dhcp-config)#**network 172.17.10.0 255.255.255.0**
R1(dhcp-config)#**default-router 172.17.10.1**
R1(dhcp-config)#**dns-server 200.48.225.130**
R1(dhcp-config)#**exit**
R1(config)# **ip dhcp excluded-address 172.17.10.1**

R2:

R2(config)#**ip dhcp pool VLAN-MATEMATICA**
R2(dhcp-config)#**network 172.17.40.0 255.255.255.0**
R2(dhcp-config)#**default-router 172.17.40.1**
R2(dhcp-config)#**dns-server 200.48.225.130**
R2(dhcp- *config*)#**exit**
R2(config)#**ip dhcp excluded-address 172.17.40.1**

R2(config)#**ip dhcp pool VLAN-FISICA**
R2(dhcp-config)#**network 172.17.30.0 255.255.255.0**
R2(dhcp-config)#**default-router 172.17.30.1**
R2(dhcp-config)#**dns-server 200.48.225.130**
R2(dhcp-config)#**exit**
R2(config)# **ip dhcp excluded-address 172.17.30.1**

TAREA 10: CONFIGURAR LOS EQUIPOS DE HOST.

Configurar las direcciones IP y gateways por defecto como se indican en la tabla de direccionamiento de las interfaces Ethernet de C3, C1, C2, C4, C6 (VPCS) y PC REAL para el correcto funcionamiento de dhcp.

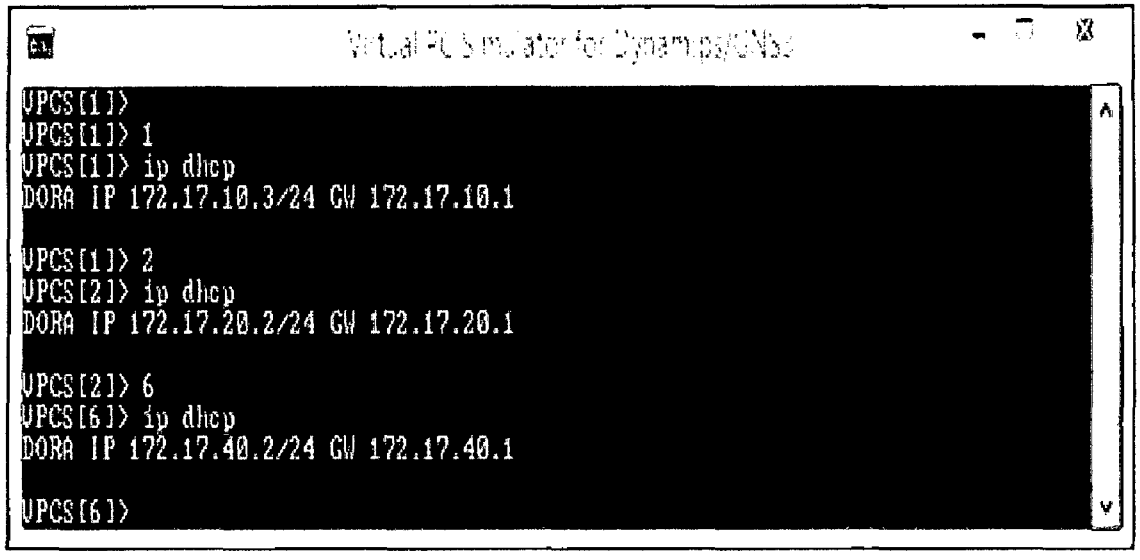


Fig. 4.8.2 Configuración de DHCP en las VPCS

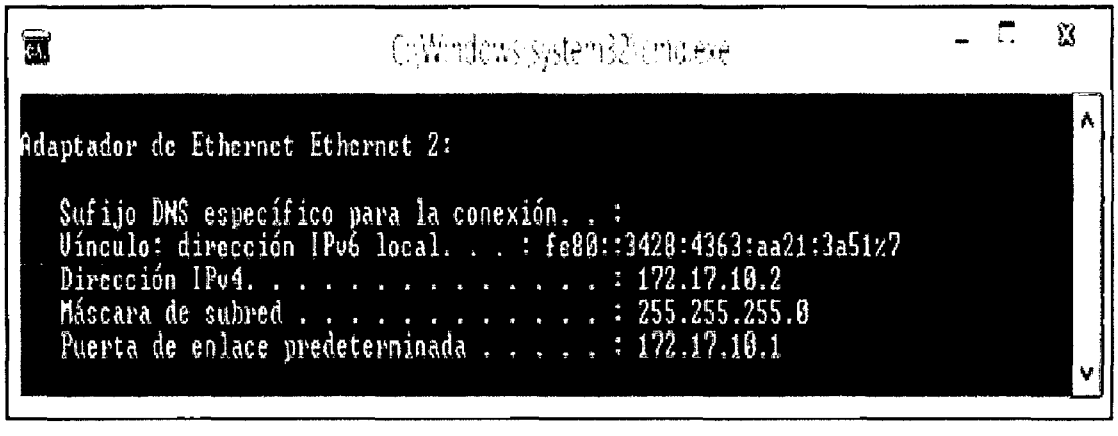


Fig. 4.8.3 Verificación de DHCP en interface bucle invertido.

TAREA 11: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

PASO 1: Verificar la configuración de VTP.

SW1#**show vtp status**

```
SW1#
SW1#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 68
Number of existing VLANs        : 7
VTP Operating Mode              : Server
VTP Domain Name                 : unprg
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x4C 0xE0 0x03 0x23 0x30 0x79 0x4D 0x52
Configuration last modified by 172.16.1.1 at 5-1-02 00:02:23
Local updater ID is 172.16.1.1 on interface Vl1 (lowest numbered VLAN interface found)
SW1#
SW1#
```

Fig. 4.8.4 Verificación de configuración de VTP en SW1

NOTA: Verificar en los demás switch la configuración vtp.

PASO 2: Verificar la creación de las VLAN en switchs y su correcta distribución a otros switch.

Use el comando **show vlan brief** en SW1 y SW4 y **show vlan-sw brief** en SW2 y SW3 para verificar que las VLAN se hayan distribuido a los switches clientes.

```
SW1#
SW1#show vlan-sw brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/5, Fa1/6, Fa1/7, Fa1/8
                                                Fa1/9, Fa1/10, Fa1/11, Fa1/12
                                                Fa1/13, Fa1/14, Fa1/15
10   vlan-electronica                 active
20   vlan-mecanica                    active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW1#
```

Fig. 4.8.5 Verificación de VLAN creadas.

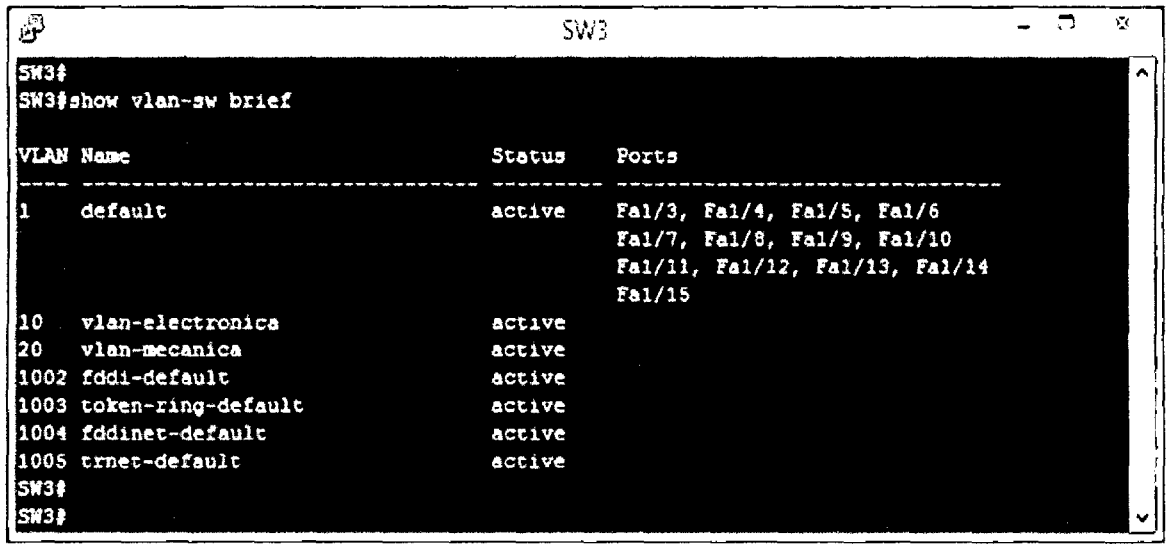


Fig. 4.7.6 Verificación de distribución de VLAN creadas.

NOTA: Verificar la distribución de las respectivas VLAN en los demás switches.

PASO 3: Verificar el direccionamiento IP y las interfaces.

R2#**show ip interface brief**

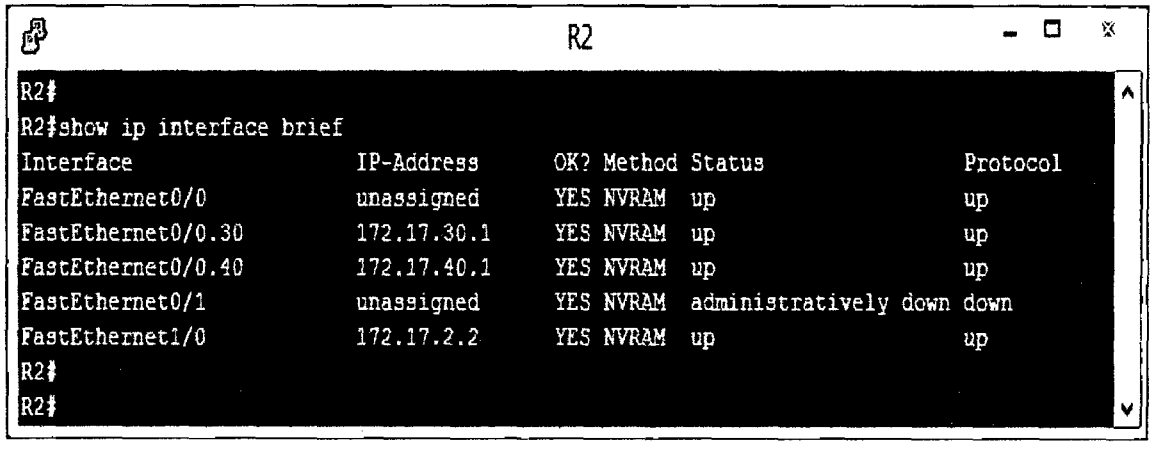


Fig. 4.8.7 Verificación de las Interfaces Activas de R2

Nota: Verificar el correcto funcionamiento de las interfaces de R1.

PASO 4: Verificar la configuración de los router. Use los comandos **show ip route** para verificar el contenido de la tabla de enrutamiento.

Desde la C1, verifique que pueda hacer ping a la PC real de la vlan30 y en los otros hosts. Puede que tome un par de pings antes de que se establezca la ruta de extremo a extremo.

R2#**show ip route**

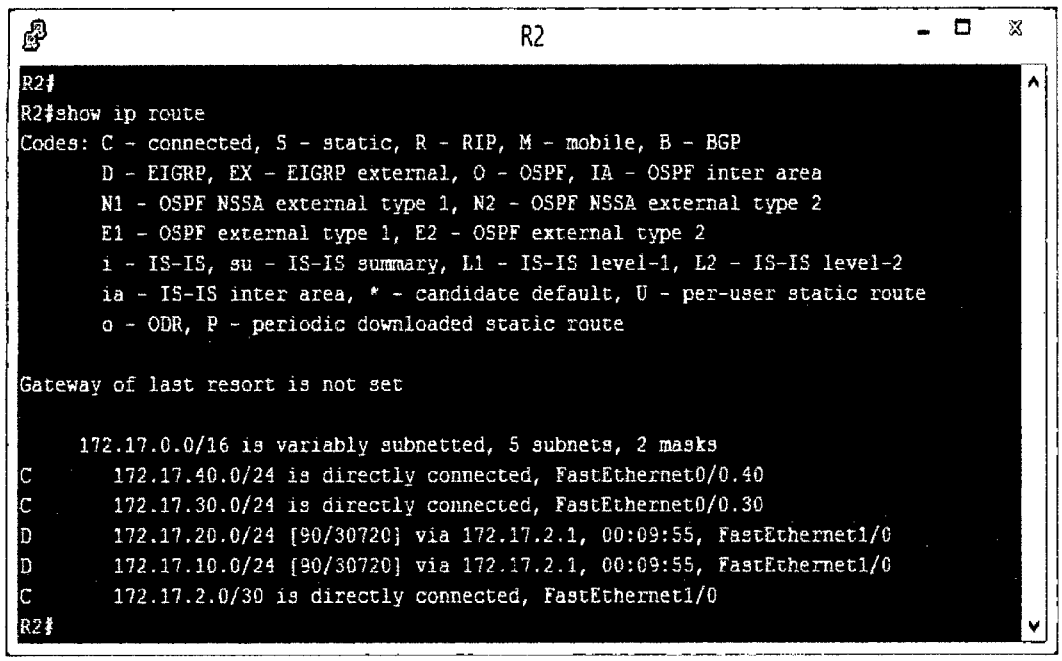


Fig. 4.8.8 Tabla de enrutamiento en R2 con EIGRP.

NOTA: Verificar la table de enrutamiento de R2.

PASO 5: Verificar la correcta configuración de Etherchannel.

SW1#**show etherchannel brief**

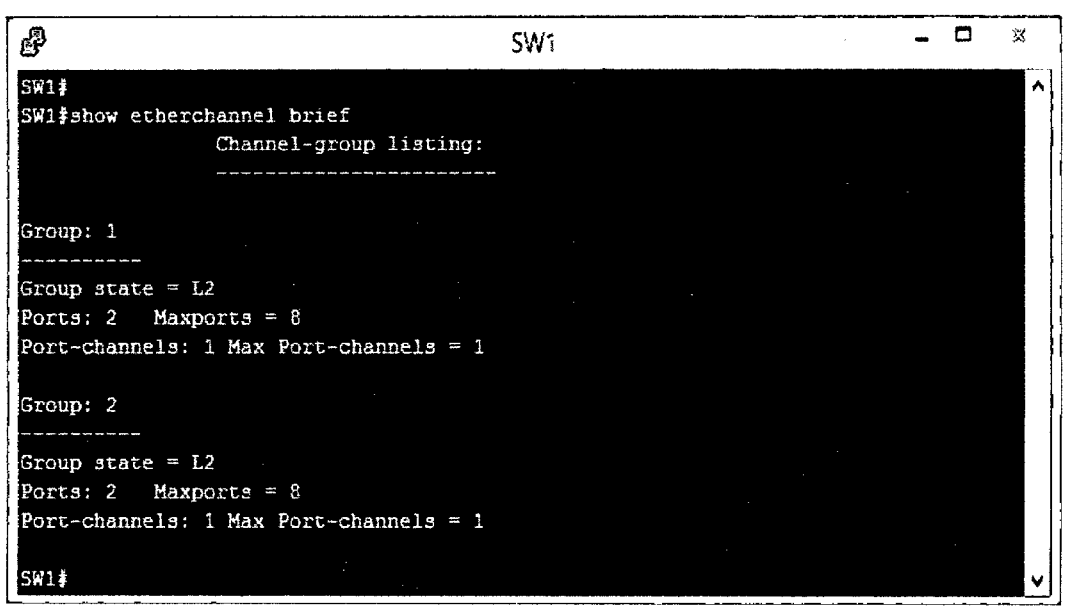


Fig. 4.8.9 Tabla de etherchannel brief.

SW1#show etherchannel summary

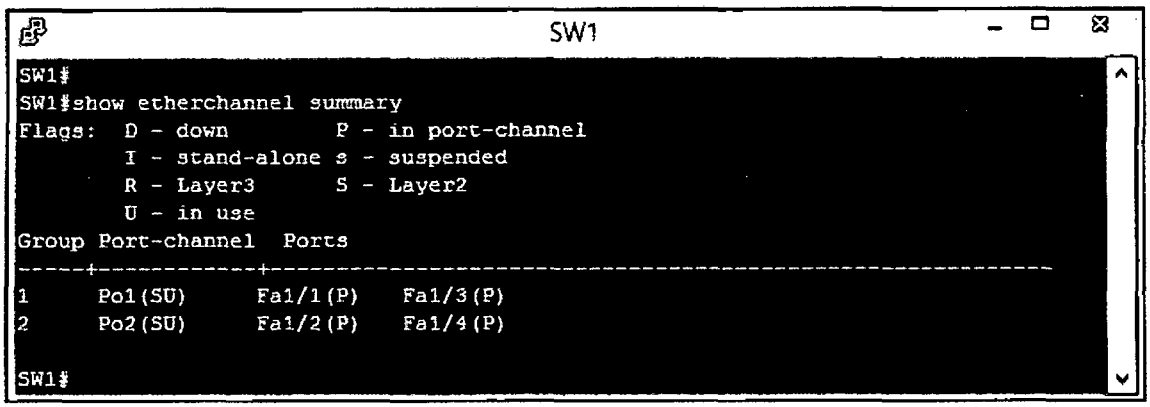


Fig. 4.8.10 Tabla de etherchannel summary.

NOTA: Verificar la correcta configuración de etherchannel en los demás switches.

PASO 6: Verificar el correcto funcionamiento de DHCP en los routers.

R1#show ip dhcp binding

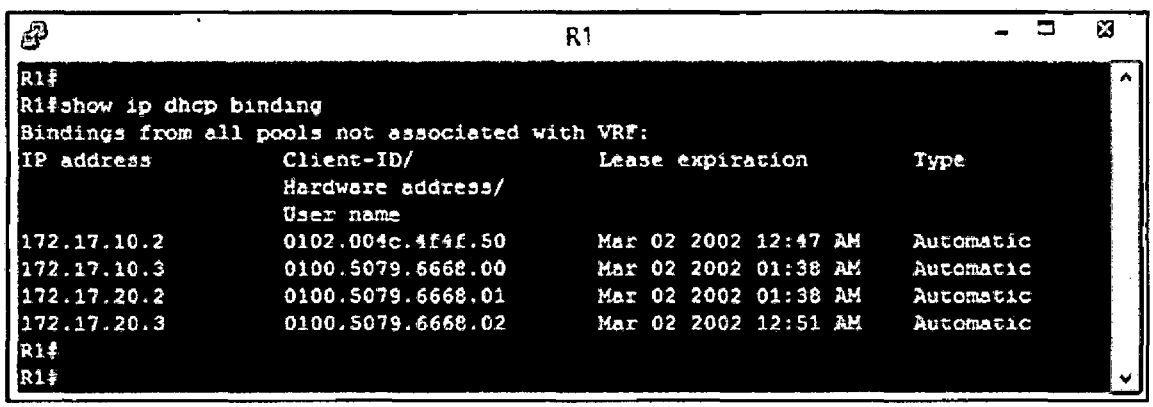


Fig. 4.8.11 Verificación de DHCP en R1.

R2#show ip dhcp binding

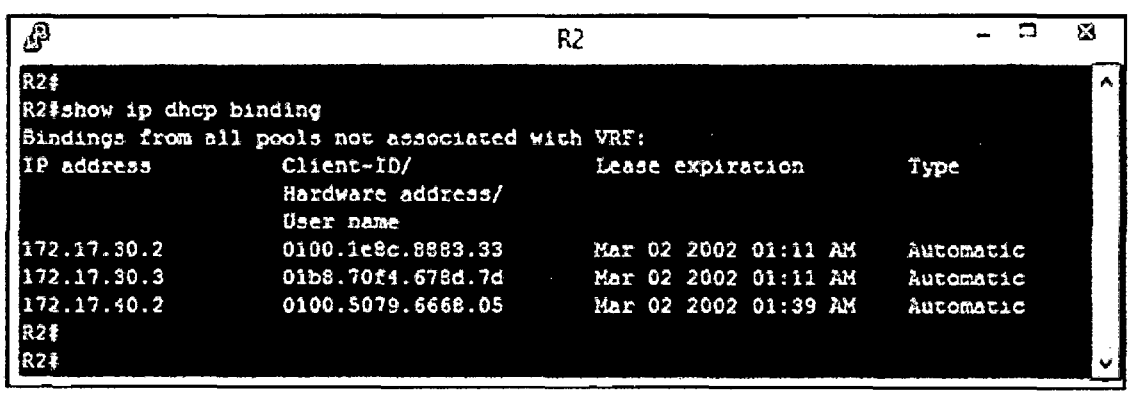


Fig. 4.8.12 Verificación de DHCP en R2.

PASO 7: Verificar que hay conectividad completa en la red.

Use el comando **ping** para verificar la conectividad.

Desde la C1, verifique que pueda hacer ping a la PC real de la vlan30 y en los otros hosts. Puede que tome un par de pings antes de que se establezca la ruta de extremo a extremo.

Verifique que todos los switches estén correctamente configurados haciendo ping entre ellos.

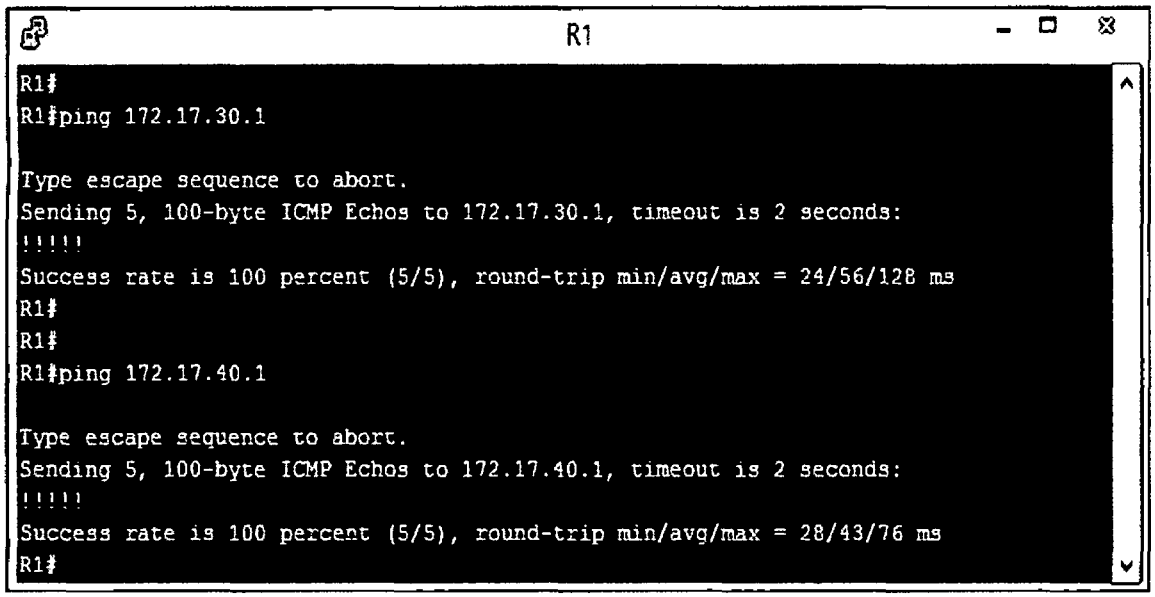


Fig. 4.8.13 Comprobación de conectividad en la red.

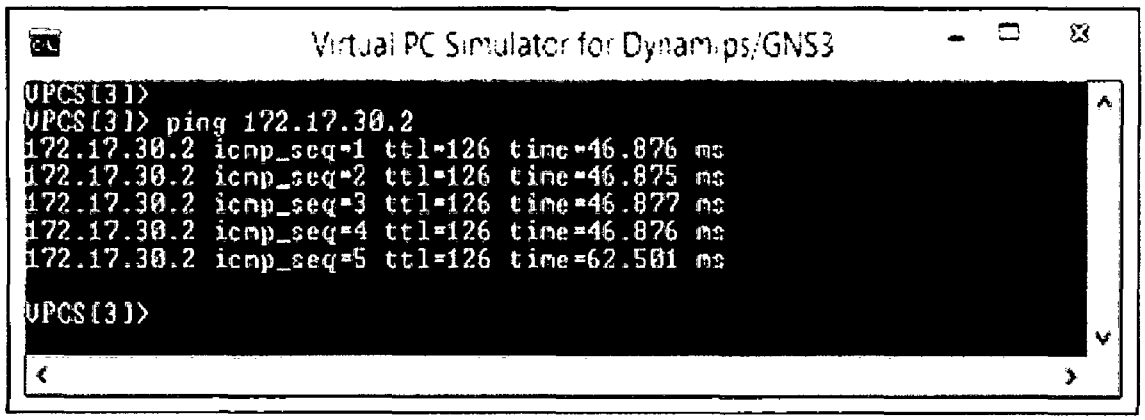


Fig. 4.8.14 Comprobación de conectividad entre C4 y PC REAL

TAREA 12: ANALIS DEL TRAFICO DE PAQUETES

PASO 1: Medición de la Latencia

Para la medición de la latencia se realizó 10 muestras sucesivas de 100 ping desde el C2 (Bucle invertido) hacia la PC REAL considerando un tamaño de trama de 64, 512 y 1518 bytes como se especifica en el RFC 2544.

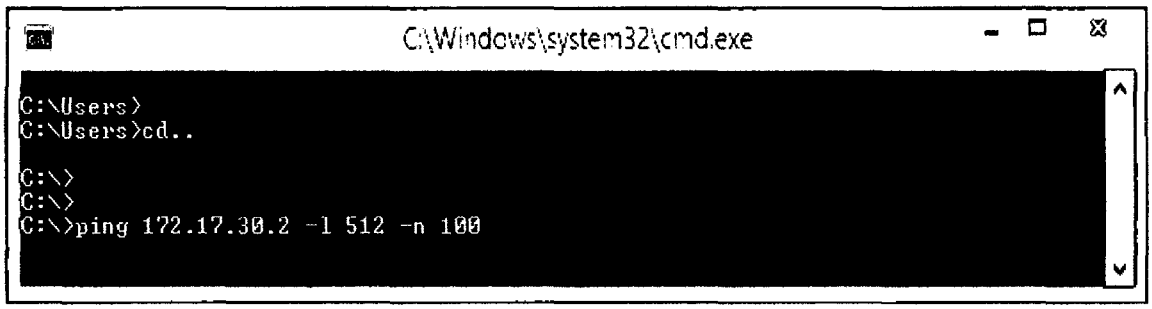


Fig. 4.8.15 Forma de medición de la Latencia.

En la Figura 4.8.15 se puede observar el envío de 100 ping con una trama de 512 hacia la dirección 172.17.30.2

En las Tablas posteriores se detallan los valores de la Latencia que se ha obtenido una vez realizadas todas las muestras.

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	N° 1	**N° 2**	**N° 3**	**N° 4**	**N° 5**	**N° 6**	**N° 7**	**N° 8**	**N° 9**	**N° 10**	**Promedio**
Tiempo Mínimo (ms)	**32**	**27**	**27**	**26**	**31**	**26**	**30**	**29**	**27**	**28**	**28.3**
Tiempo Máximo (ms)	**329**	**214**	**233**	**164**	**303**	**170**	**248**	**221**	**194**	**199**	**227.5**
Tiempo Promedio (ms)	**145**	**107**	**116**	**73**	**99**	**87**	**85**	**102**	**77**	**100**	**99.1**

Tabla 4.8.9 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	512										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	33	30	27	32	27	23	28	32	31	31	29.4
Tiempo Máximo (ms)	422	441	226	262	198	244	197	226	240	206	266.2
Tiempo Promedio (ms)	166	153	85	97	74	80	81	77	118	73	118.4

Tabla 4.8.10 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1518										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	29	30	30	29	30	29	32	29	30	33	30.1
Tiempo Máximo (ms)	354	396	296	322	297	304	305	258	364	287	318.3
Tiempo Promedio (ms)	80	127	125	120	160	155	166	118	126	120	129.7

Tabla 4.8.11 Datos obtenidos para una trama de 1518 bytes.

LATENCIA			
Tamaño de Trama (bytes)	64	512	1518
Tiempo Mínimo (ms)	28.3	29.4	30.1
Tiempo Máximo (ms)	227.5	266.2	318.3
Tiempo Promedio (ms)	99.1	118.4	129.7

Tabla 4.8.12 Comparación de datos obtenidos de las diferentes tramas.

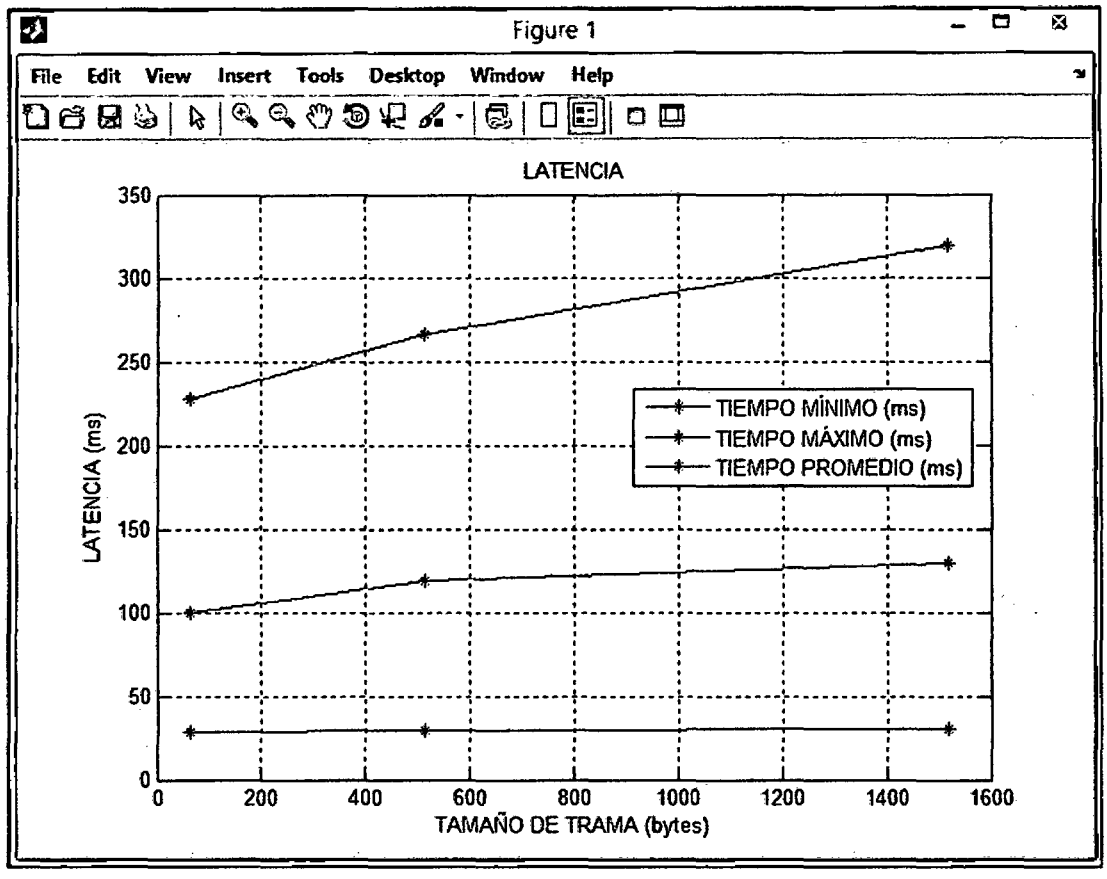


Fig. 4.8.16 Datos representados gráficamente de la variación de la latencia.

De acuerdo con los datos obtenidos, se puede observar claramente que los valores mínimo (color azul), máximo (color rojo) y promedio (color verde) de la latencia de la red se incrementan conforme se envía una trama de longitud mayor, en este caso con la trama de 1518 bytes se obtiene una latencia promedio de 129.7 ms a diferencia de una trama de 64 bytes con 99.1 ms.

PASO 2: Medición del Throughput

Para la medición del Throughput y Jitter se envió una cantidad de tramas a velocidades diferentes durante 20 segundos, hasta encontrar la máxima cantidad de tramas recibidas sin que se produzcan perdidas de las mismas en el router y PC REAL. Como se utilizó Jperf el cliente será el encargado de enviar los paquetes y el servidor los recibirá, indicando la cantidad de paquetes que llegaron correctamente considerando un tamaño del paquete UDP de 750, 1125, 1500 y 1470 (default) bytes, tal como se especifica en el RFC 768.

Configuración del Jperf como servidor para medir Throughput:

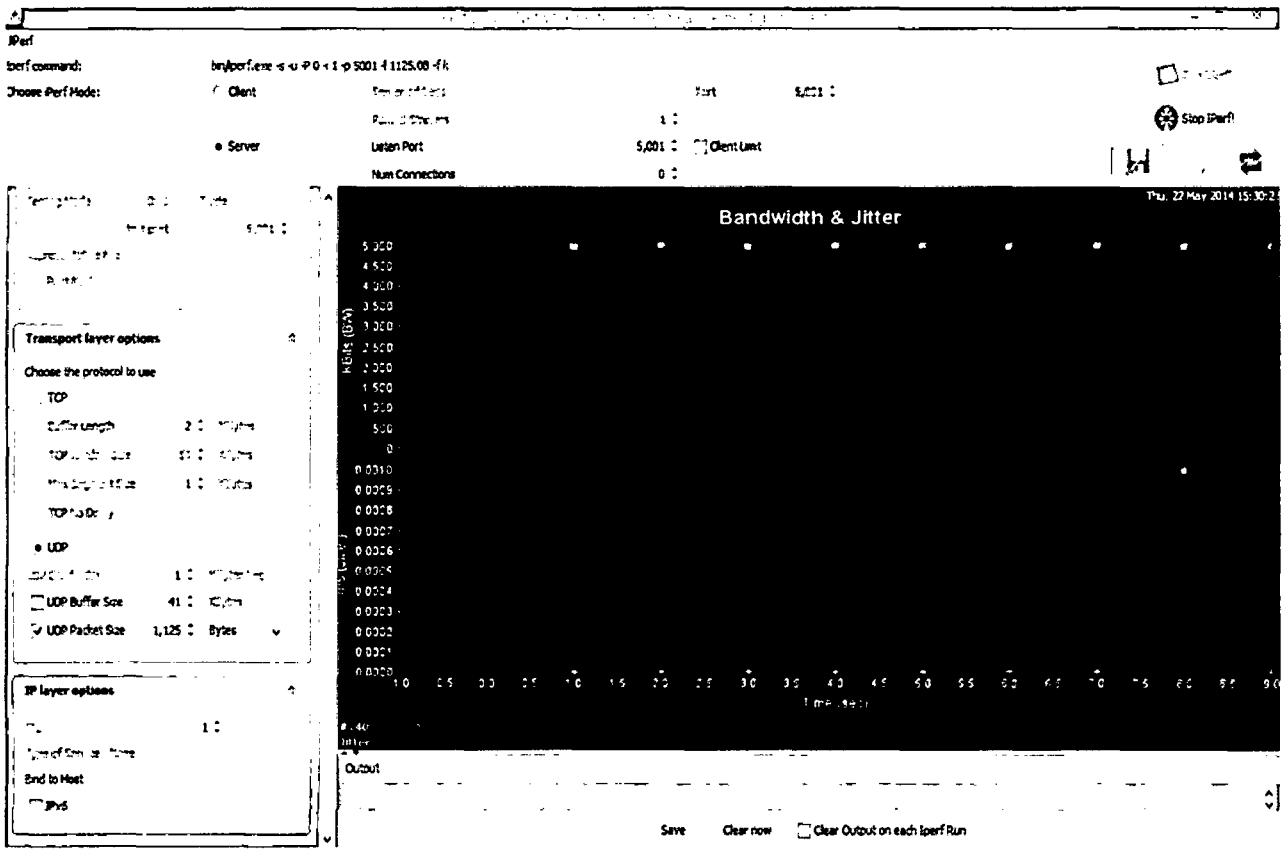


Fig. 4.8.17 Gráfico del Bandwidth y Jitter en Jperf.

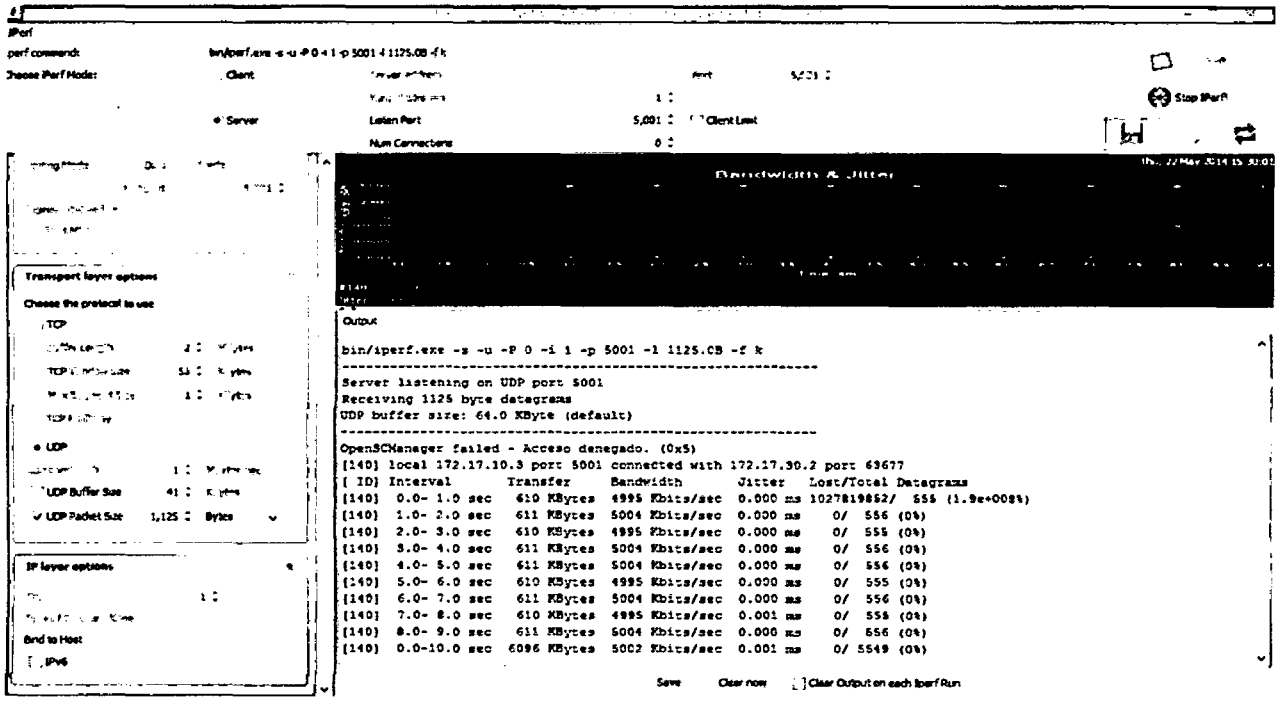


Fig. 4.8.18 Configuración del Jperf como Servidor para medir Jitter.

Configuración del Jperf como cliente para medir Throughput:

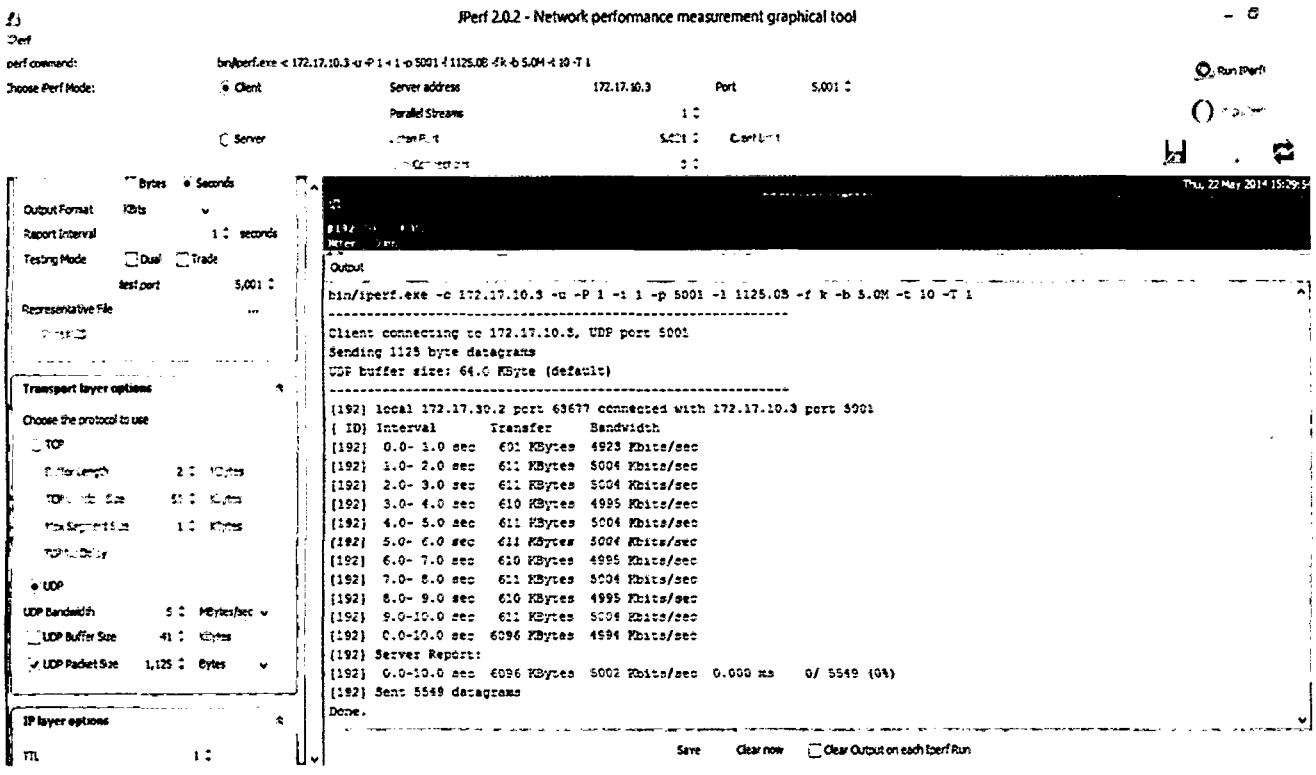


Fig. 4.8.19 Configuración del Jperf como Cliente para medir Throughput.

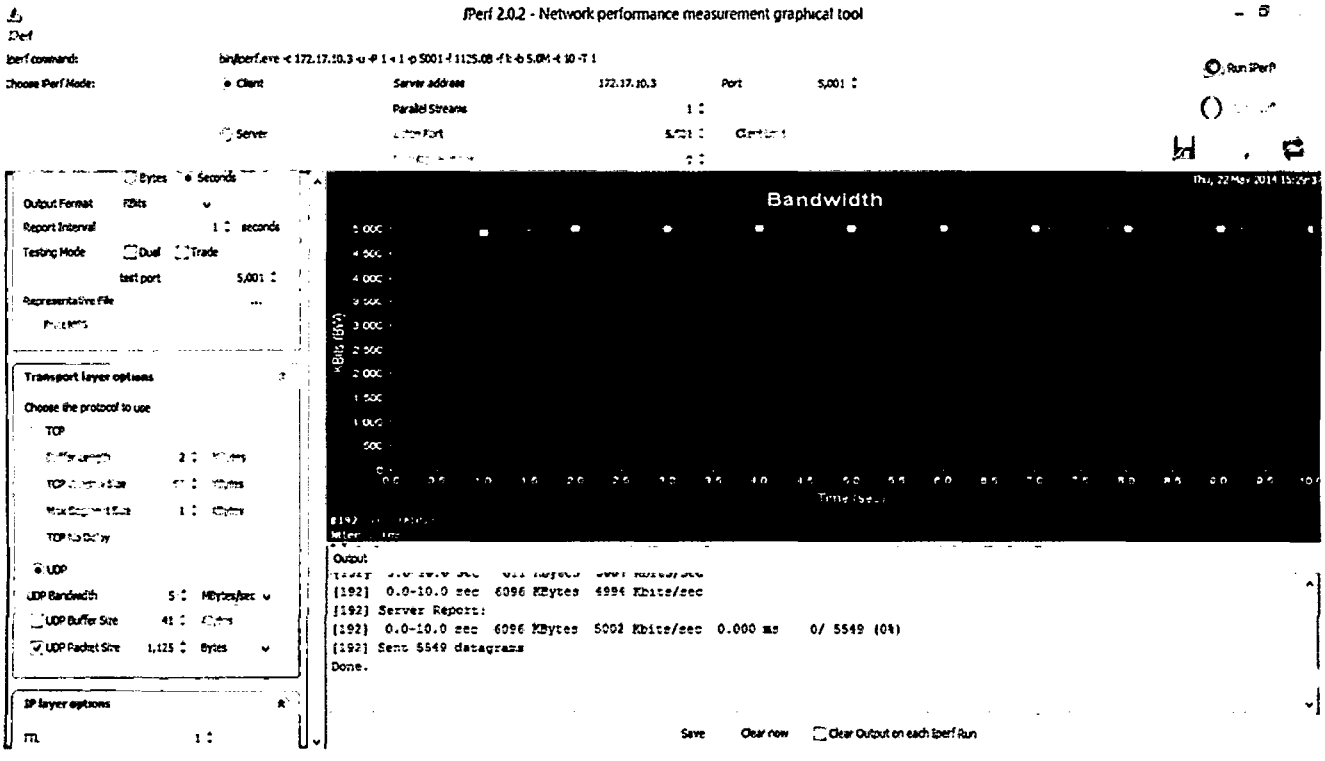


Fig. 4.8.20 Gráfico del Bandwidth en Jperf.

En las siguientes Tablas se detalla los valores del Throughput obtenidos una vez realizada todas las muestras.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**5**	**5**	**5**
Velocidad de Rx (Mbps)	**5**	**5**	**5**
Tramas Transmitidas	**8327**	**5549**	**4163**
Tramas Recibidas	**8327**	**5549**	**4163**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**833**	**555**	**416**

Tabla 4.8.13 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**2**	**5**	**8**
Velocidad de Rx (Mbps)	**2**	**4.99**	**7.98**
Tramas Transmitidas	**1700**	**4249**	**6794**
Tramas Recibidas	**1700**	**4249**	**6794**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**170**	**425**	**680**

Tabla 4.8.14 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

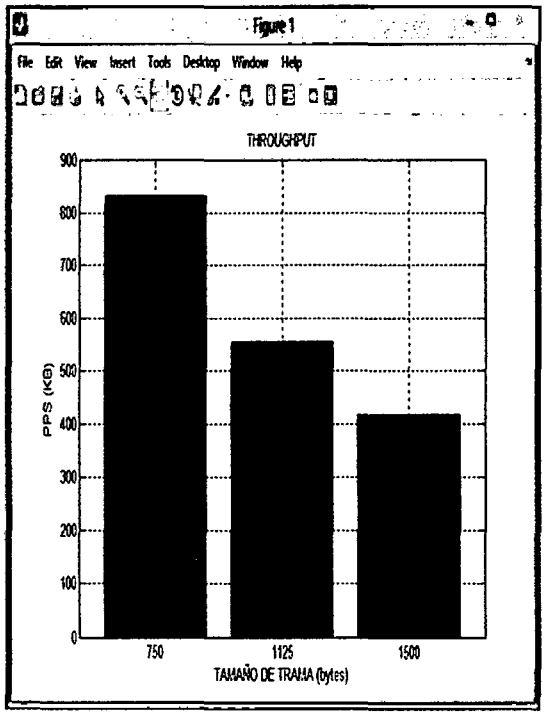


Fig. 4.8.21 PPS vs. Tamaño de Trama

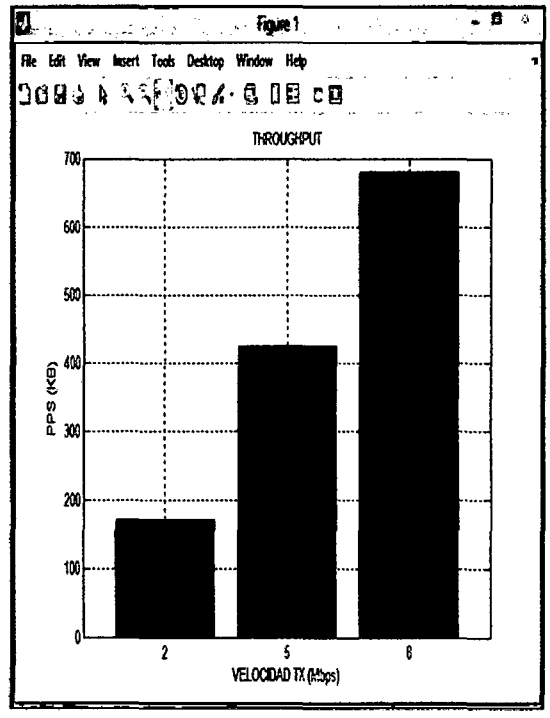


Fig. 4.8.22 PPS vs. Velocidad Tx

En la figura 4.8.21, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 750 bytes, 1125 bytes y 1500 bytes los cuales han utilizado una velocidad de Tx constante de 5 Mbps, en la gráfica se puede observar claramente que al enviar una trama de 750 bytes se envía 833 pps, con una trama de 1125 se envía 555 pps y con una trama de 1500 se envía 418 pps.

Mientras en la figura 4.8.22, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 1470 bytes los cuales han utilizado una velocidad de Tx variada desde 2 Mbps hasta 8 Mbps sin que se produzcan perdidas en el envío, en la gráfica se observa que a 2 Mbps se envían 170 pps, en cambio a 8 Mbps se obtiene 680 pps.

PASO 3: Medición del Jitter

Para la medición se envió datos UDP de longitud variable a velocidades diferentes de Throughput obtenida anteriormente durante 20 segundos. Como se utilizó anteriormente Jperf el cliente será el encargado de enviar los datos y el servidor los recibirá, indicando los valores de Jitter obtenidos durante la transmisión de los datos.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**5**	**5**	**5**
Velocidad de Rx (Mbps)	**5**	**5**	**5**
Tramas Transmitidas	**8327**	**5549**	**4163**
Tramas Recibidas	**8327**	**5549**	**4163**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**0.004**	**0.001**	**0**

Tabla 4.8.15 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**2**	**5**	**8**
Velocidad de Rx (Mbps)	**2**	**4.99**	**7.98**
Tramas Transmitidas	**1700**	**4249**	**6794**
Tramas Recibidas	**1700**	**4249**	**6794**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**0.001**	**0**	**0**

Tabla 4.8.16 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

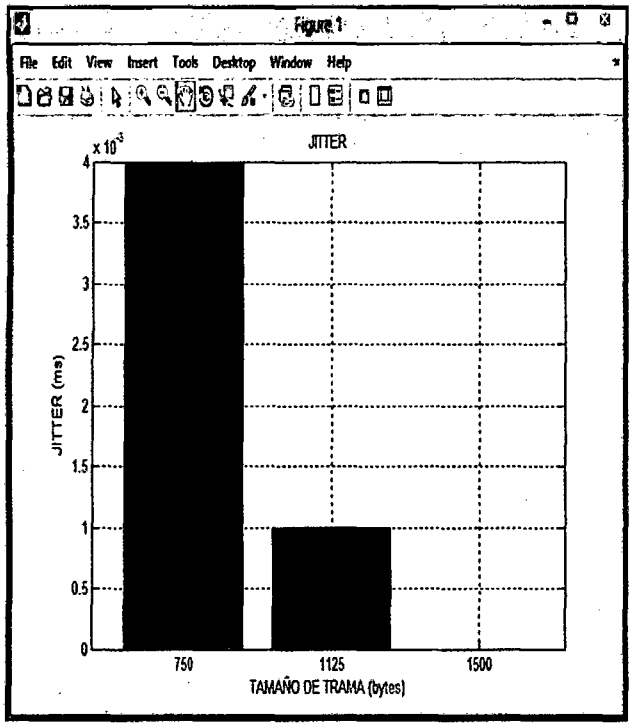


Fig. 4.8.23 Jitter vs. Tamaño de Trama

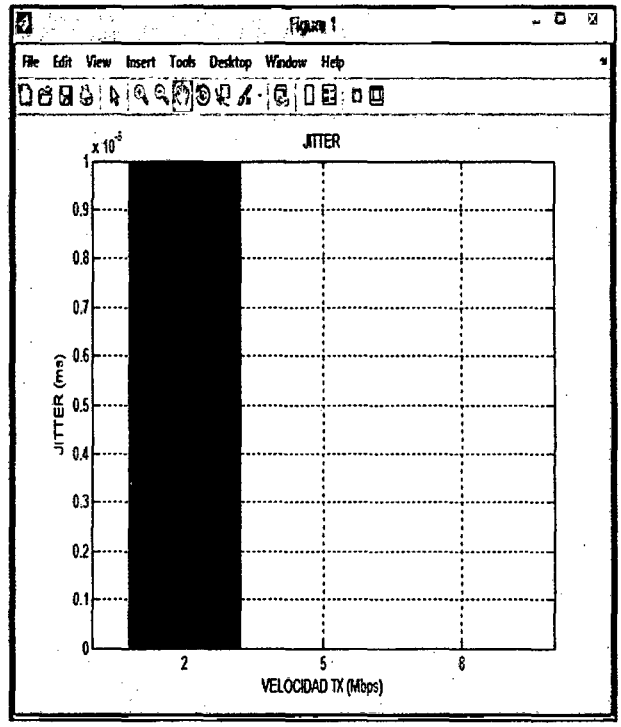


Fig. 4.8.24 Jitter vs. Velocidad Tx

En la figura 4.8.23 se observa los valores del Jitter obtenidos al enviar diferentes tamaños de paquete UDP como 750, 1125 y 1500 bytes utilizando una velocidad de Tx constante de 5 Mbps, se puede observar claramente que con una trama de 750 bytes se tiene un Jitter de 0.004 ms a diferencia de la trama de 1500 bytes en la cual se tiene un Jitter de 0 ms.

En la figura 4.8.24, se observa los valores del Jitter obtenidos al enviar paquetes UDP de 1470 bytes utilizando una velocidad de Tx que varía entre los 2 Mbps y los 8 Mbps, se puede observar claramente que con una velocidad Tx de 2 Mbps se tiene un Jitter de 0.001 ms a diferencia que a una velocidad Tx de 8 Mbps en la cual se tiene un Jitter de 0 ms.

Medición de Jitter a 5 Mbps:

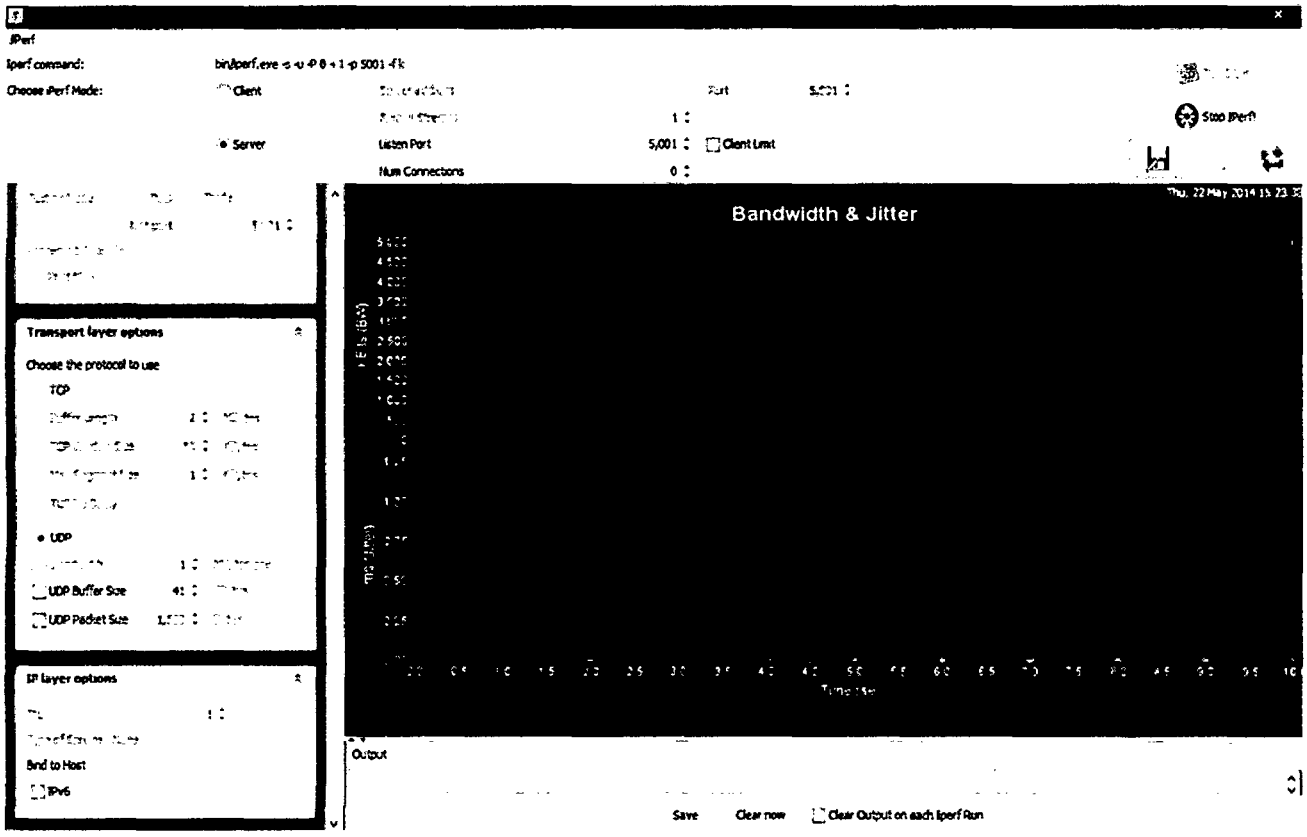


Fig. 4.8.25 Gráfica de Bandwidth y Jitter.

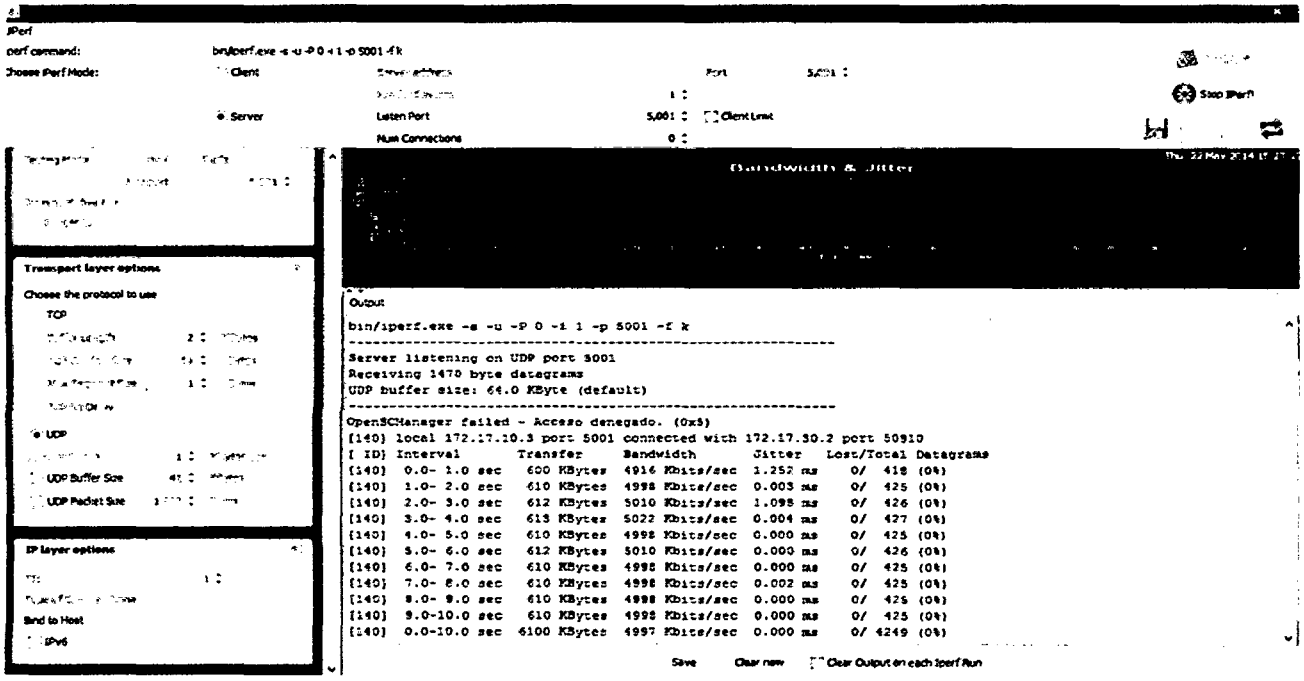


Fig. 4.8.26 Resultados al medir Throughput como servidor.

PASO 4: Captura de tráfico con Wireshark.

Capturar tráfico de paquetes en la interfaz f1/0 de R1.

- Captura de paquetes ICMP.

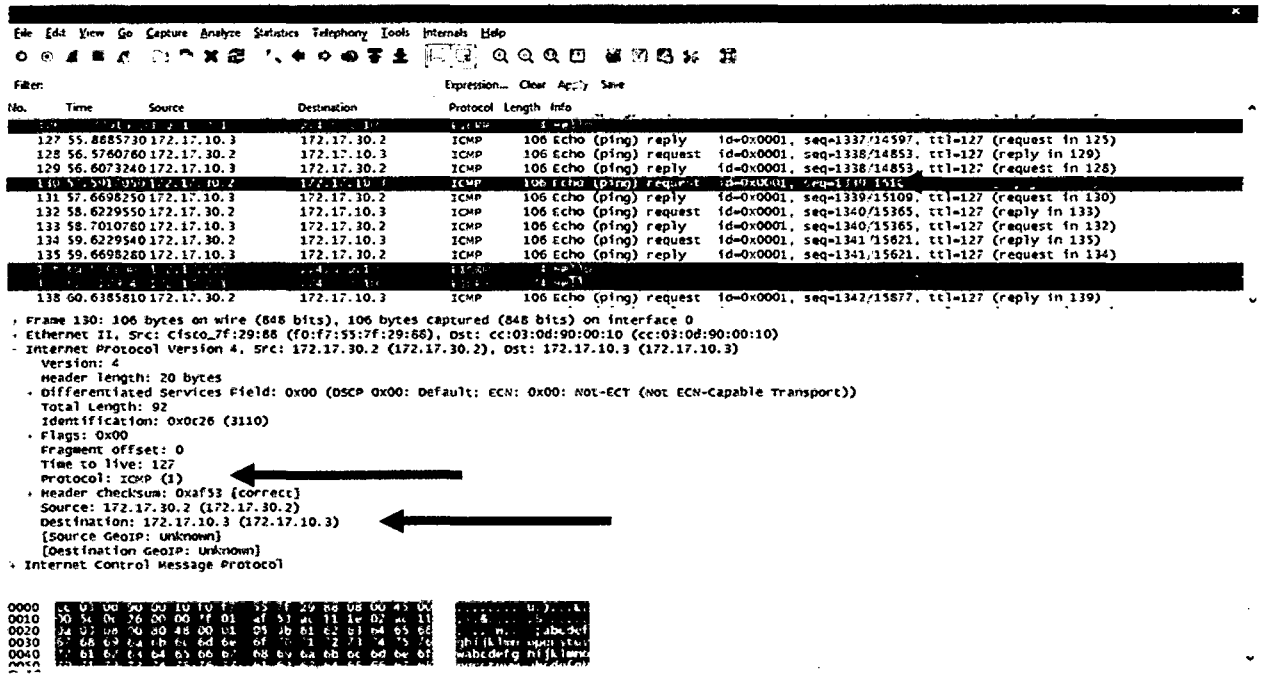


Fig. 4.8.27 Captura de tráfico en la red con Wireshark.

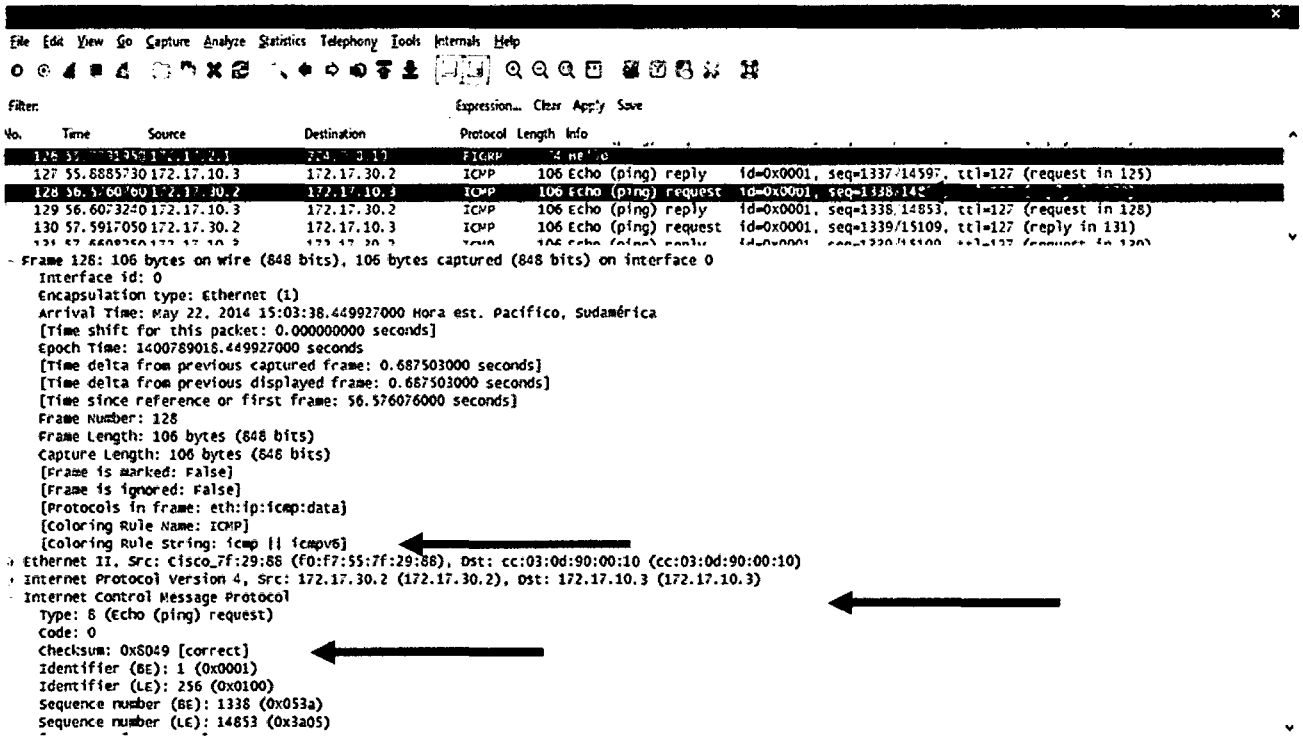


Fig. 4.8.28 Información detallada del paquete ICMP.

- Protocolo de enrutamiento EIGRP:

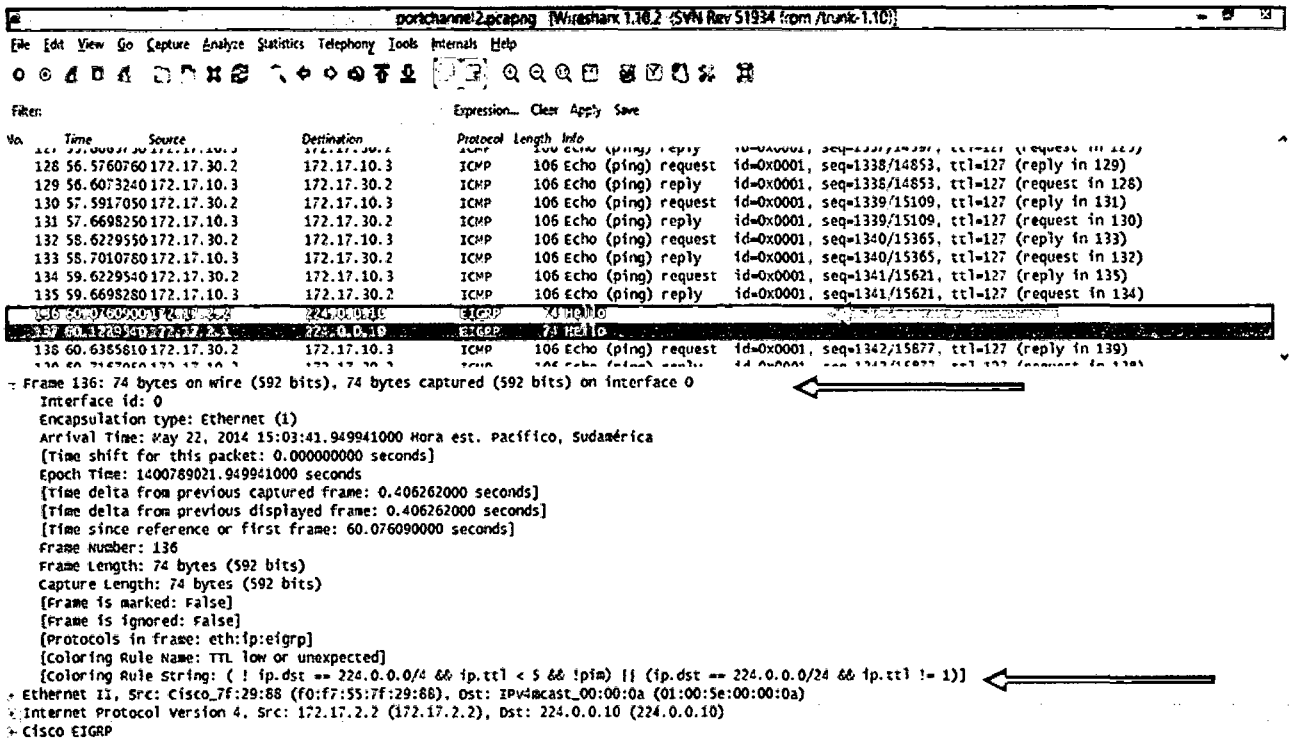


Fig. 4.8.29 Captura del protocolo OSPF con Wireshark.

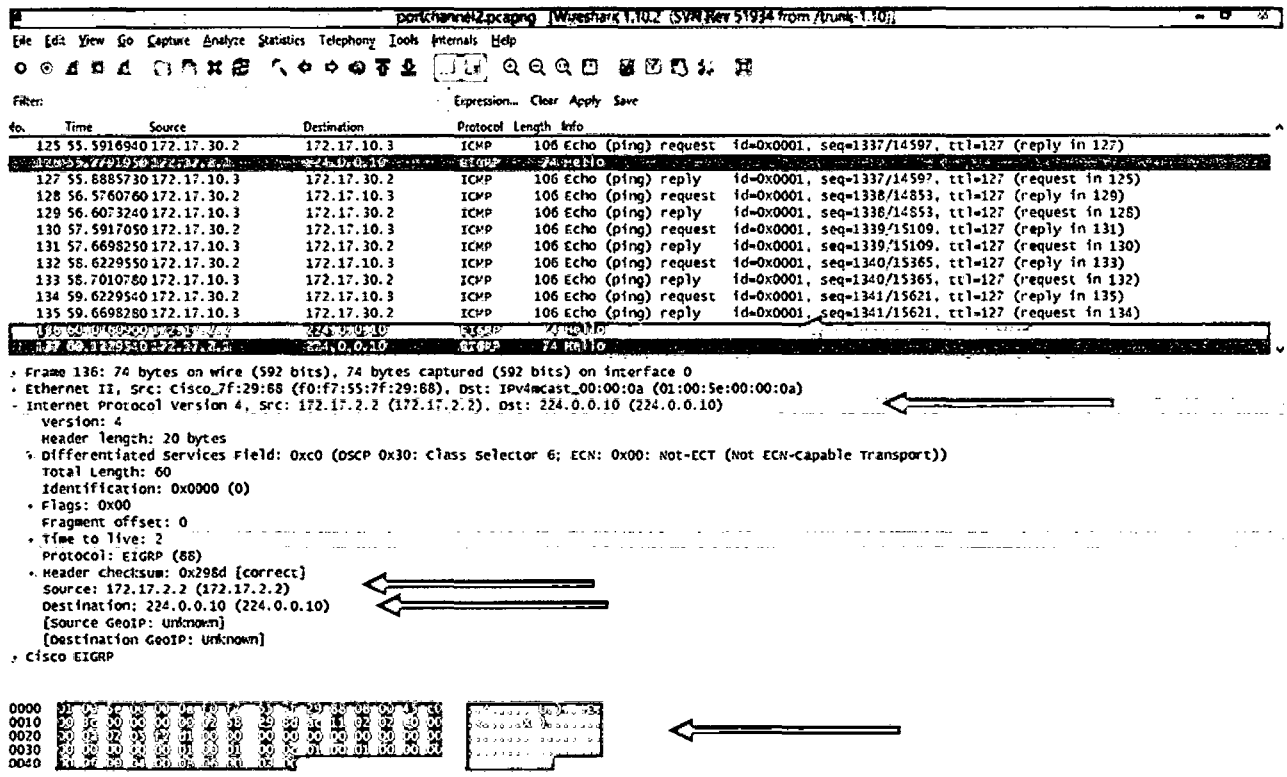


Fig. 4.8.30 Información detallada del protocolo EIGRP.

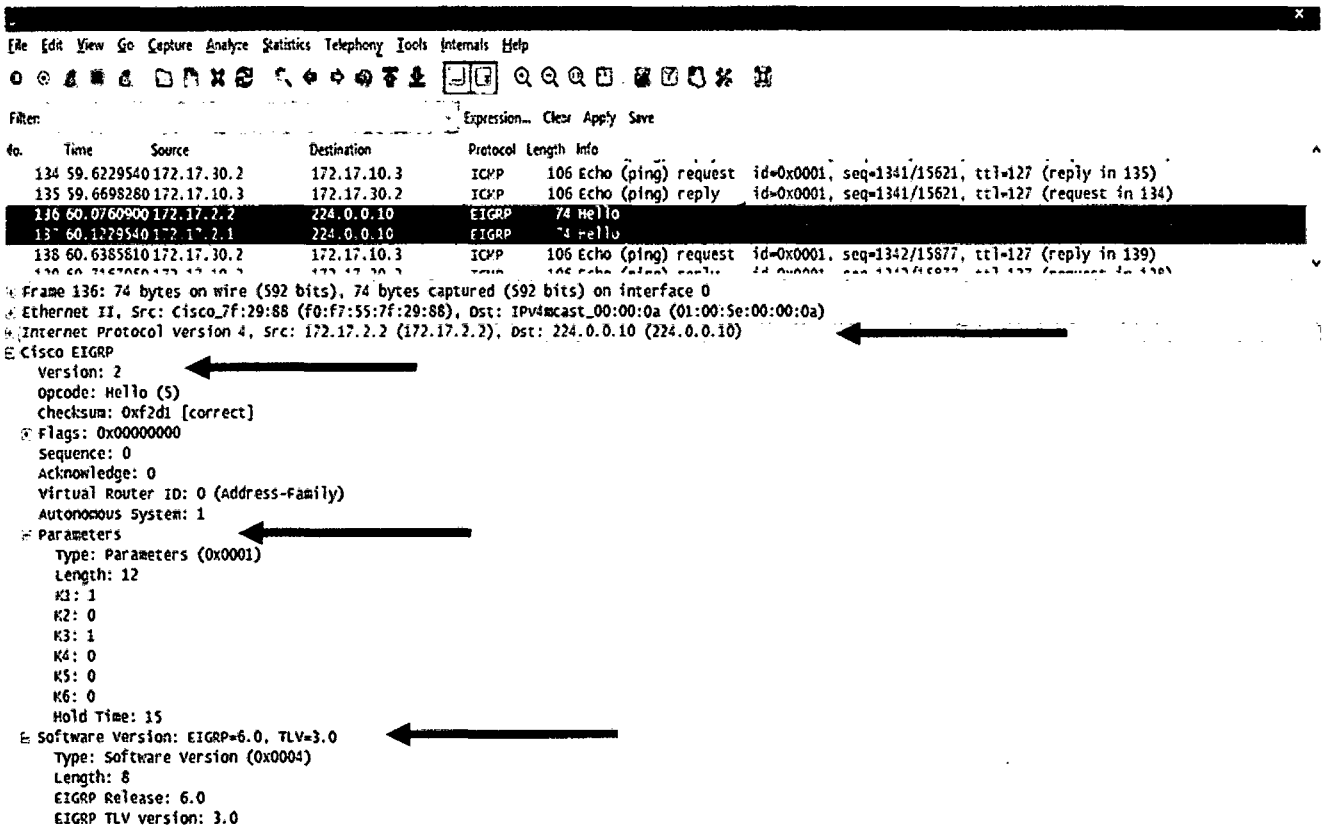


Fig. 4.8.31 Información detallada del protocolo EIGRP.

LABORATORIO 4.9: VOIP

REVISIÓN TEÓRICA: Para la realización de esta práctica se deberá revisar conceptos de VOIP.

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet.
- Configurar VOIP.
- Configurar el enrutamiento OSPF.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **192.168.1.0/30** entre el router **R1-R2**, además teniendo las siguientes redes:

LAN R1: 192.168.10.0/24
LAN R2: 192.168.20.0/24

DIAGRAMA DE TOPOLOGIA

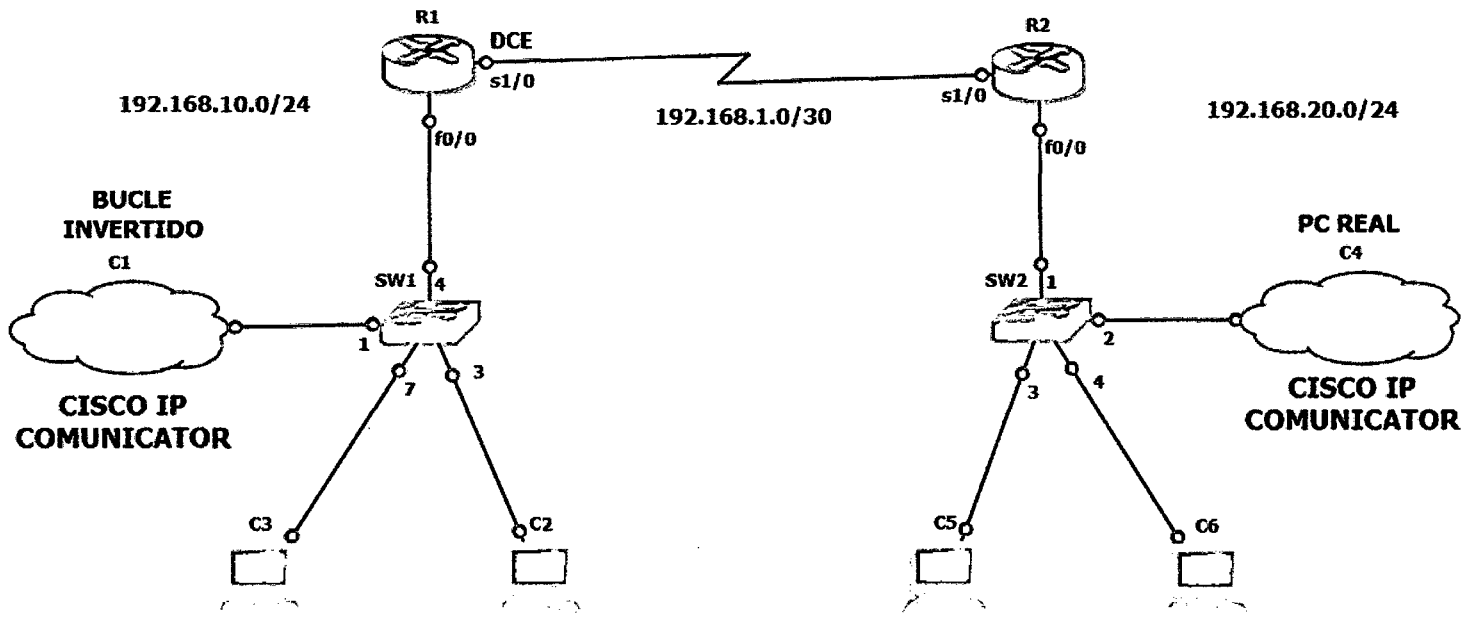


Fig. 4.9.1 Red Virtual en GNS3

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	f0/0	192.168.10.1	255.255.255.0	No aplicable
	s1/0	192.168.1.1	255.255.255.252	No aplicable
R2	f0/0	192.168.20.1	255.255.255.0	No aplicable
	s1/0	192.168.1.2	255.255.255.252	No aplicable
C1	BUCLE INVERTIDO	DHCP	DHCP	DHCP
C2	VPCS	DHCP	DHCP	DHCP
C3	VPCS	DHCP	DHCP	DHCP
C4	NIC	DHCP	DHCP	DHCP
C5	VPCS	DHCP	DHCP	DHCP
C6	VPCS	DHCP	DHCP	DHCP

Tabla 4.9.1 Direccionamiento IP para las Redes

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

Montar y conectar la red igual a la del Diagrama de topología.

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

Ingrese al modo privilegiado

Router>enable

Aparece el siguiente prompt

Router#

En el modo exec privilegiado, ingrese al modo de configuración global:

Router# **configure terminal**

PASO 1: Establezca la configuración global del nombre de host.

Ingrese el siguiente comando para configurar el nombre del router:

Router(config)#**hostname XXXXXX** (Escribir nombre deseado)

PASO 2: Desactive la búsqueda DNS.

Router(config)# **no ip-domain lookup**

Si escribes algo que no sea un comando de Cisco IOS o cometes un error, el router asume que ha escrito un nombre de dominio y trata de resolver lo que usted escribe, realizando una búsqueda de DNS.

PASO 3: Configure un mensaje para que se muestre al ingresar al router.

Router(config)#**banner motd %** Solo acceso a personal autorizado **%** (Puede escribir cualquier mensaje)

El símbolo % indica el inicio y final del mensaje.

PASO 4: Configure las contraseñas de consola, enable secret y VTY.

Seguir los siguientes pasos:

Router(config)# **line console 0**

Router(config-line)# **password XXXXX** (Escribir contraseña deseada)

Router(config-line)# **login**

Router(config-line)# **exit**

Router(config)# **enable secret XXXXX** (Escribir contraseña deseada)

Router(config)# **line vty 0 4**

Router(config-line)# **password XXXXX** (Escribir contraseña deseada)

Router(config-line)# **login**

Router(config-line)# **exit**

PASO 5: Sincronice los mensajes no solicitados y el resultado de la depuración con el resultado solicitado y los indicadores para las líneas de consola y de terminal virtual.

Router(config)# **line console 0**

Router(config)# **logging synchronous**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **logging synchronous**

Router(config)# **exit**

PASO 6: Configure un tiempo de espera EXEC de 10 minutos.

Router(config)# **line console 0**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

PASO 7: Guardar la configuración.

Router(config)# **copy running-config startup-config**

TAREA 3: CONFIGURAR INTERFACES, DHCP Y SERVICIO DE TELEFONIA.

PASO 1: configure y active las interfaces fastethernet y seriales.

R1:

R1(config)# **interface s1/0**

R1(config-if)# **description conexion a R2**

R1(config-if)# **ip address 192.168.1.1 255.255.255.252**

R1(config-if)# **clock rate 64000**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface f0/0**

R1(config-if)# **description conexion a SW1**

R1(config-if)# **ip address 192.168.10.1 255.255.255.0**

R1(config-if)# **no shutdown**

R2:

R2(config)# **interface s0/0**

R2 (config-if)# **description conexion a R1**

R2 (config-if)# **ip address 192.168.1.2 255.255.255.252**

R2 (config-if)# **no shutdown**

R2 (config-if)# **exit**

R2 (config)# **interface f0/0**

R2 (config-if)# **description conexion a SW2**

R2 (config-if)# **ip address 192.168.20.1 255.255.255.0**

R2 (config-if)# **no shutdown**

PASO 2: Configurar dhcp.

R1(config)# **ip dhcp pool A**

R1(dhcp-config)# **network 192.168.10.0 255.255.255.0**

R1(dhcp-config)# **default-router 192.168.10.1**

R1(dhcp-config)#**option 150 ip 192.168.10.1**

R1(dhcp-config)# **exit**

R1(config)# **ip dhcp excluded-address 192.168.10.1**

NOTA: seguir los mismos pasos para crear dhcp pool B en R2.

PASO 3: Editar el servicio de telefonía.

R1(config)# **telephony-service**

R1(config-telephony)# **max-dn 2**

R1(config-telephony)# **max-ephones 2**

R1(config-telephony)# **ip source-address 192.168.10.1 port 2000**

R1(config-telephony)# **auto assign 4 to 6**

R1(config-telephony)# **auto assign 1 to 5**

R1(config-telephony)# **exit**

R1(config)# **ephone-dn 1**

R1(config-ephone-dn)# **number 100**

R1(config-ephone-dn)# **end**

NOTA: Seguir los mismos pasos para R2 con sus respectivos parámetros, asignando el número 200 para el teléfono IP.

TAREA 4: CONFIGURAR EIGRP.

R1:

R1(config)# **router eigrp 1**

R1(config-router)# **network 192.168.1.0 0.0.0.3 area 0**

R1(config-router)# **network 192.168.10.0 0.0.0.255 area 0**

R1(config-router)# **exit**

R2:

R2(config)# **router eigrp 1**

R2(config-router)# **network 192.168.1.0 0.0.0.3 area 0**

R2(config-router)# **network 192.168.20.0 0.0.0.255 area 0**

R2(config-router)# **exit**

TAREA 5: CONFIGURAR DIAL-PEER.

R1:

R1(config)# **dial-peer voice 1 voip**

R1(config-dial-peer)# **dial-peer voice 1 voip** (ID del enrutador VOIP)

R1(config-dial-peer)# **destination-pattern 200** (Número de destino: 200)

R1(config-dial-peer)# **session target ipv4: 192.168.1.2** (IP del router VOIP vecino)

R2:

R2(config)# **dial-peer voice 1 voip**

R2(config-dial-peer)# **dial-peer voice 1 voip**

R2(config-dial-peer)# **destination-pattern 100**

R2(config-dial-peer)# **session target ipv4: 192.168.1.1**

TAREA 6: CONFIGURAR LOS EQUIPOS DE HOST.

VPCS

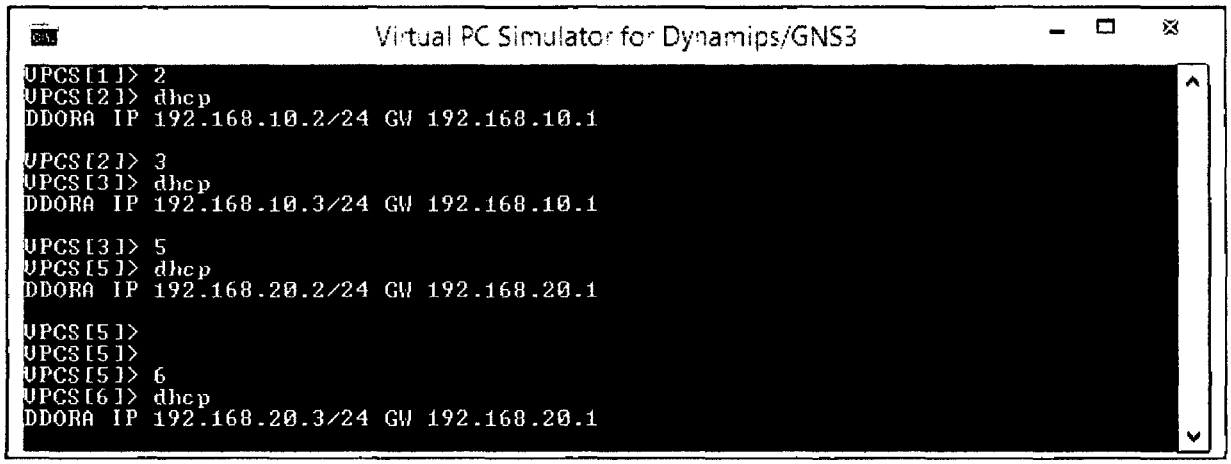


Fig. 4.9.2 Dirección IP de las VPCS.

BUCLE INVERTIDO

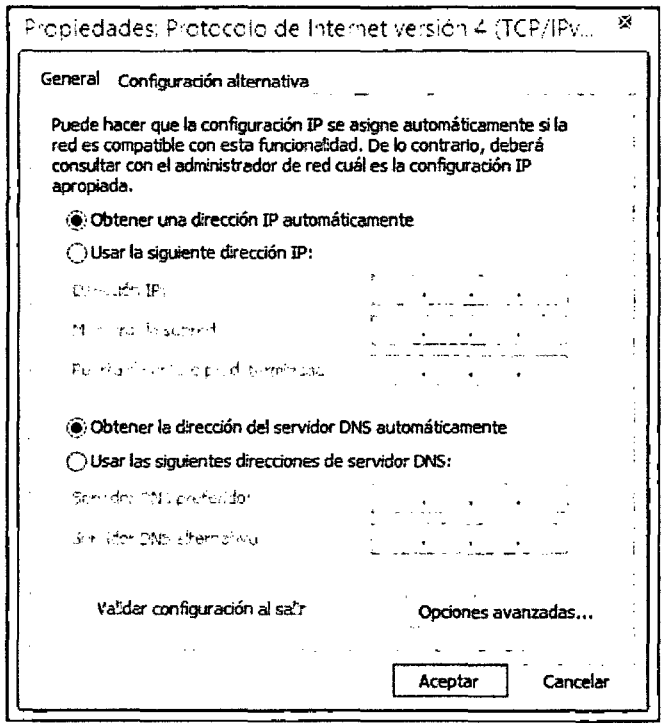


Fig. 4.9.3 Configuración de Bucle invertido.

NOTA: Configurar en Cisco IP Comunicator las preferencias.

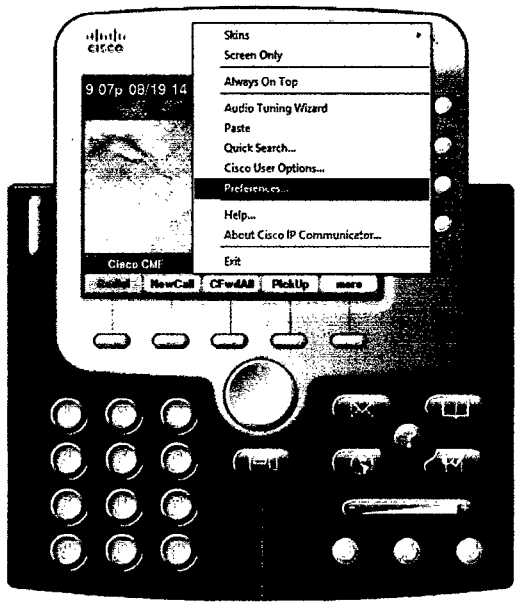
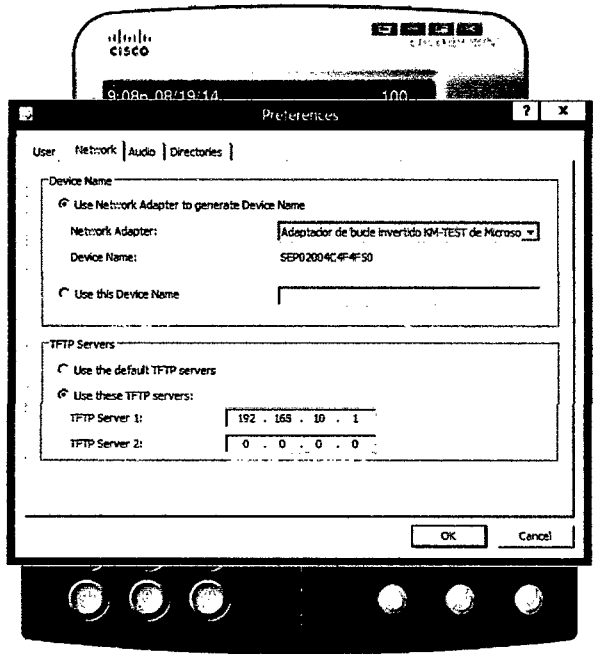


Fig. 4.9.4 Configuración Cisco IP Comunicator.



NOTA: Colocar la dirección IP del Servidor.

Fig. 4.9.5 Dirección IP del servidor.

TAREA 7: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

PASO 1: Revisar si los teléfonos IP recibieron los números correspondientes:

PC REAL-NIC **BUCLE INVERTIDO**

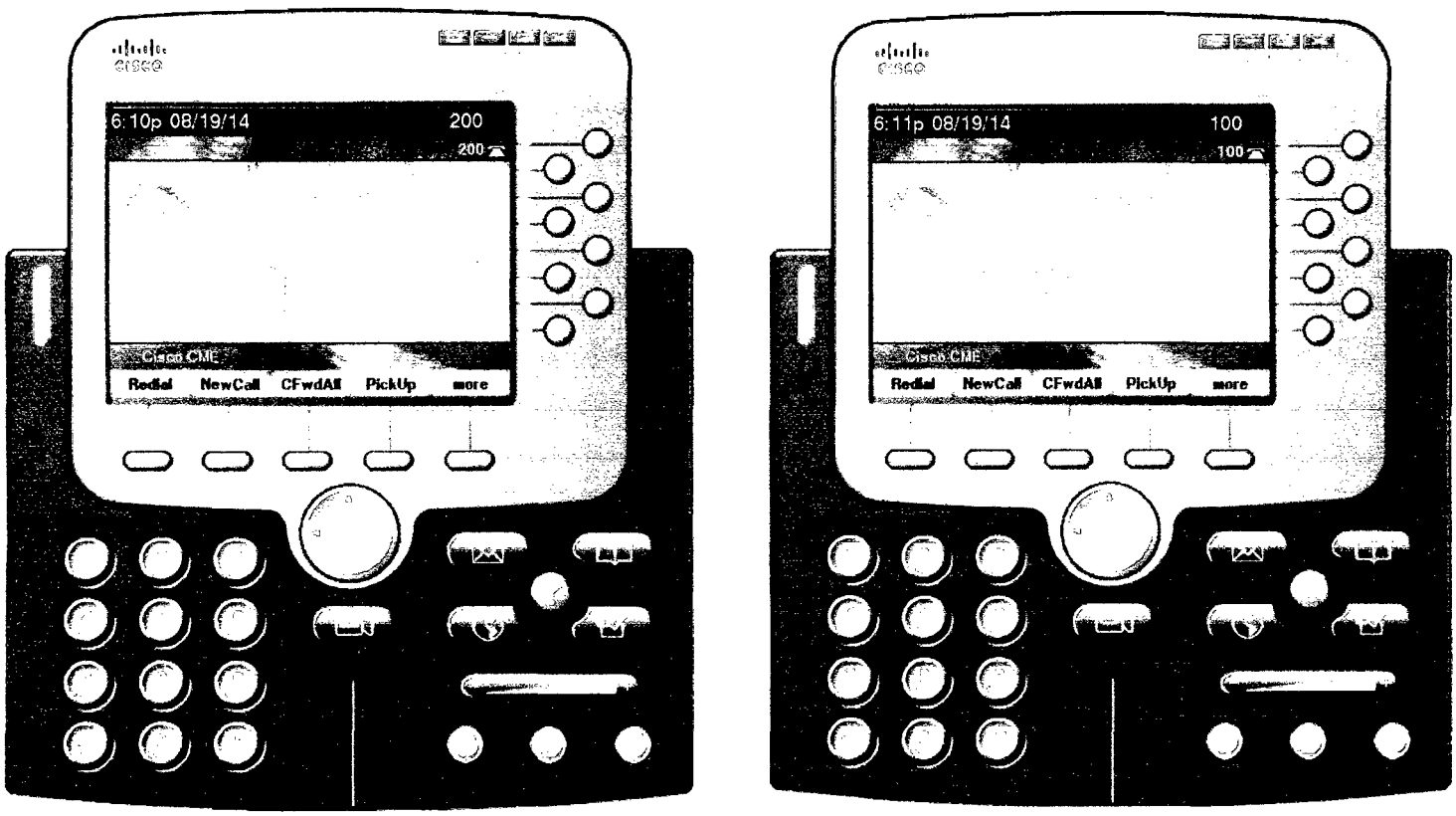


Fig. 4.9.6 Asignación de IP a teléfonos.

PASO 2: Realizar una llamada para comprobar la comunicación:

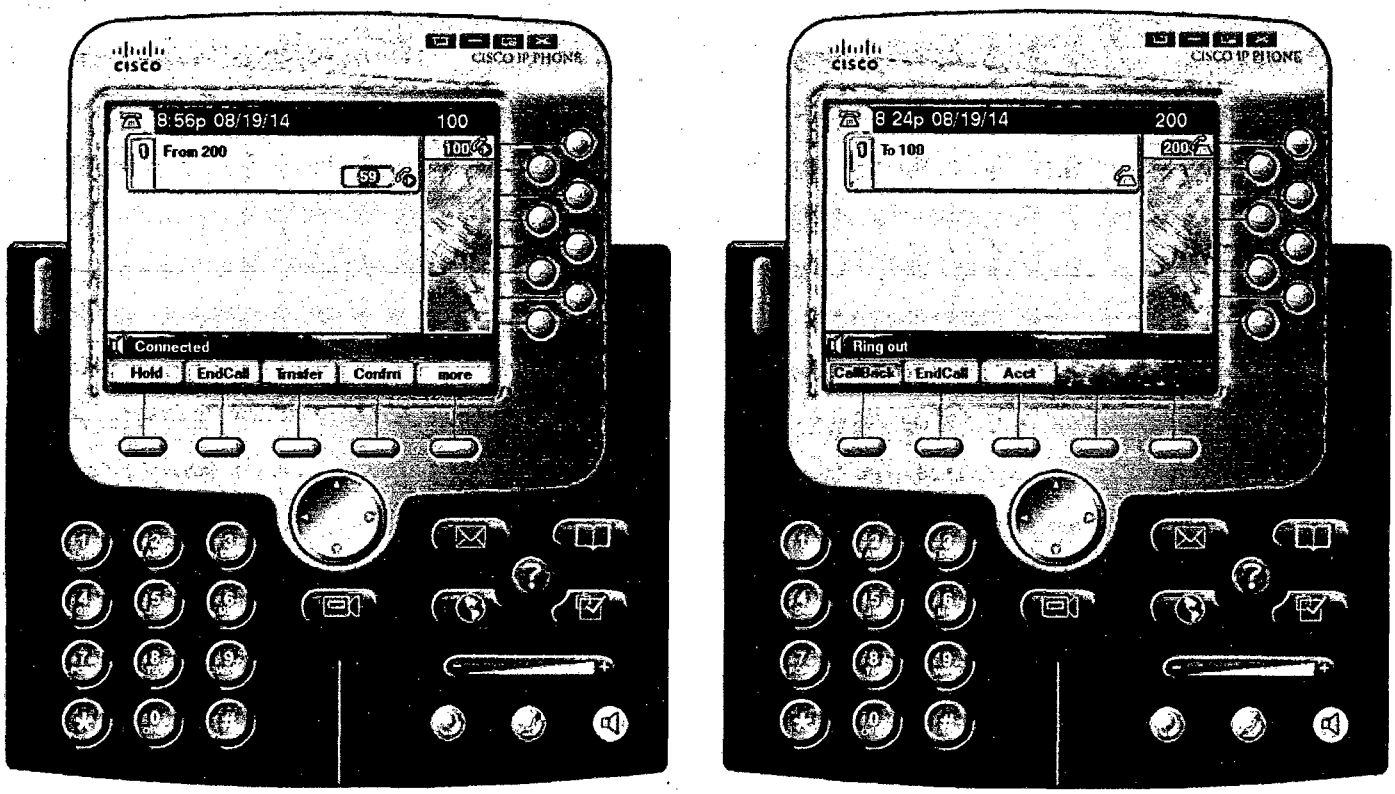


Fig. 4.9.7 Comprobación de llamada.

TAREA 8: ANALIS DEL TRAFICO DE PAQUETES

WIRESHARK

PASO 1: Se capturaran datos en la interface f0/0 de R1:

- Se observan los paquetes **HELLO EIGRP.**

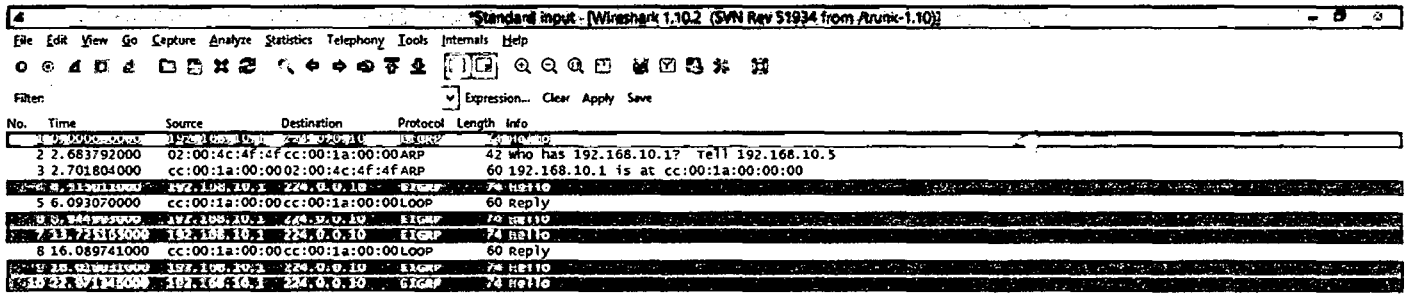


Fig. 4.9.8 Captura de paquete HELLO EIGRP con Wireshark

En esta imagen se puede observar con más detalles los parámetros del protocolo de enrutamiento EIGRP y también el campo del paquete HELLO.

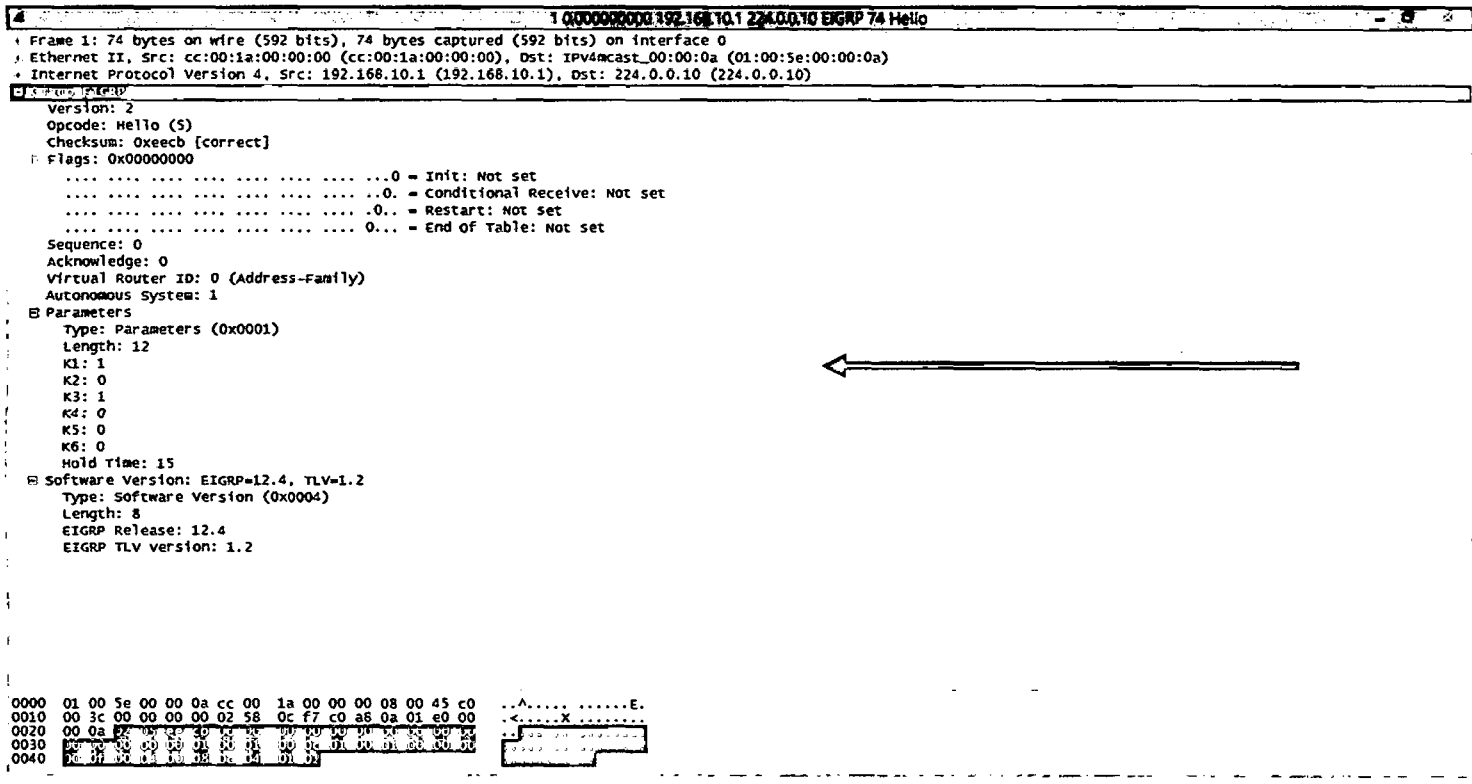


Fig. 4.9.9 Información detallada del paquete HELLO EIGRP.

- También se capturan los paquetes de mensajes **Skinny Client Control Protocol**, el cual es un protocolo ligero que permite una comunicación eficiente con un sistema Cisco Call Manager.

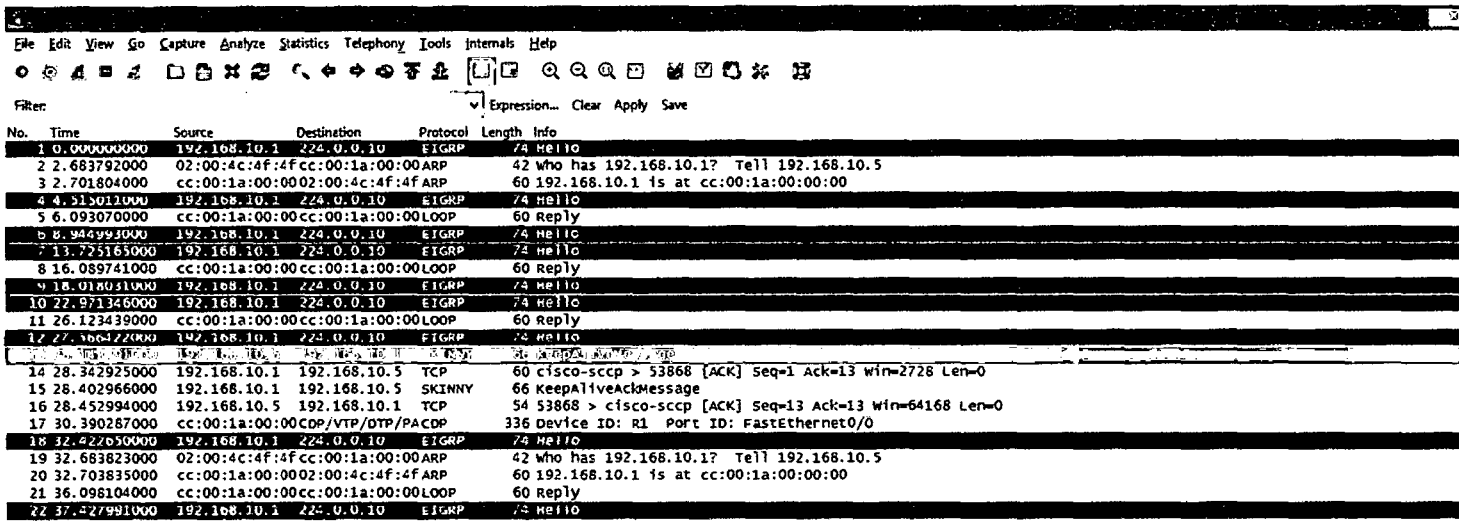
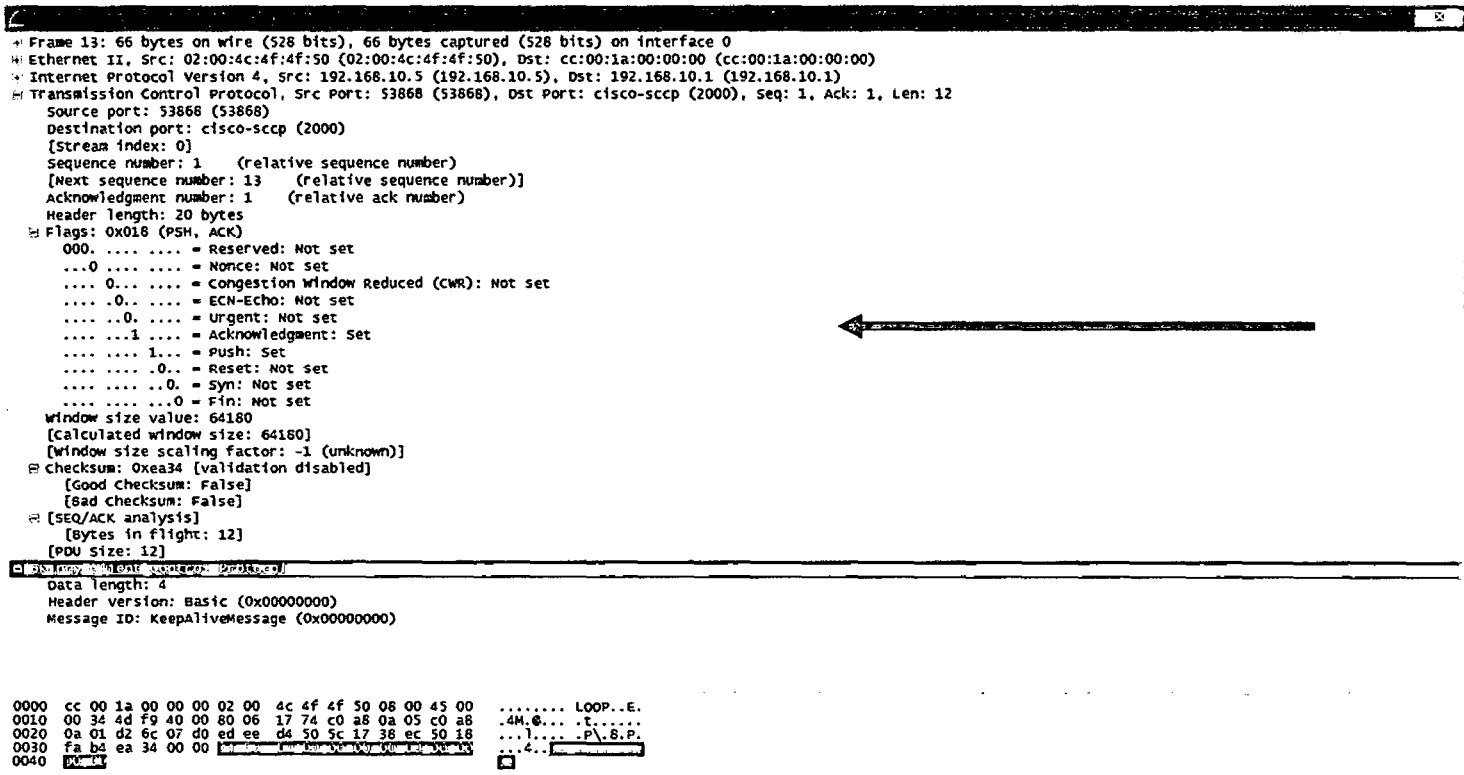


Fig. 4.9.10 Captura de paquete SKINNY con Wireshark.

En esta imagen se puede analizar con más detalles los diversos campos del mensaje



Skinny.

Fig. 4.9.11 Informacion detallada del paquete SKINNY.

- Al realizar una llamada observamos el tráfico de paquetes **RTP**, el cual es un protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real, como por ejemplo audio y vídeo en una video-conferencia.

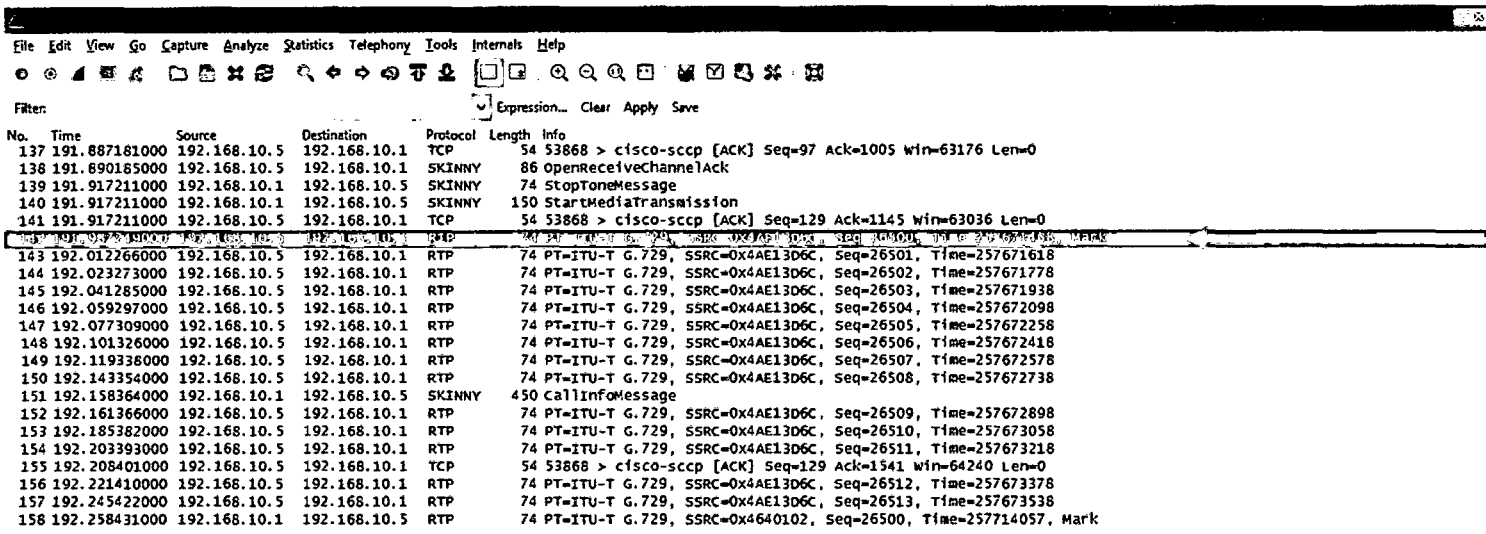


Fig. 4.9.12 Captura de paquete RTP con Wireshark

En la siguiente imagen se puede observar más detalladamente:

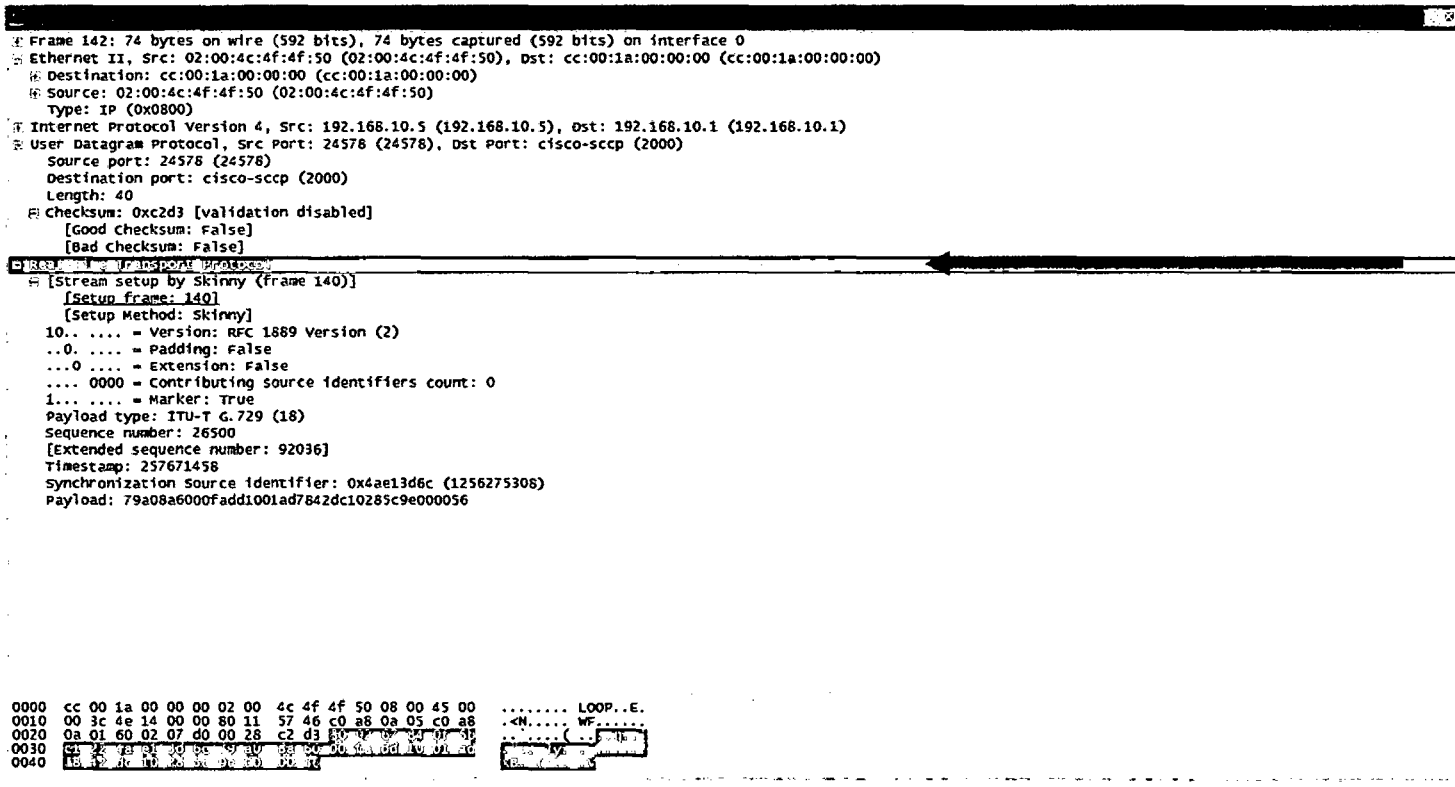


Fig. 4.9.13 Información detallada del paquete RTP.

PASO 2: Se capturaran datos en la interface s0/0 de R1:

- Se capturan paquetes de **H.225.0**, protocolo de comunicaciones utilizados comúnmente para voz sobre IP y para videoconferencia basada en el protocolo IP.

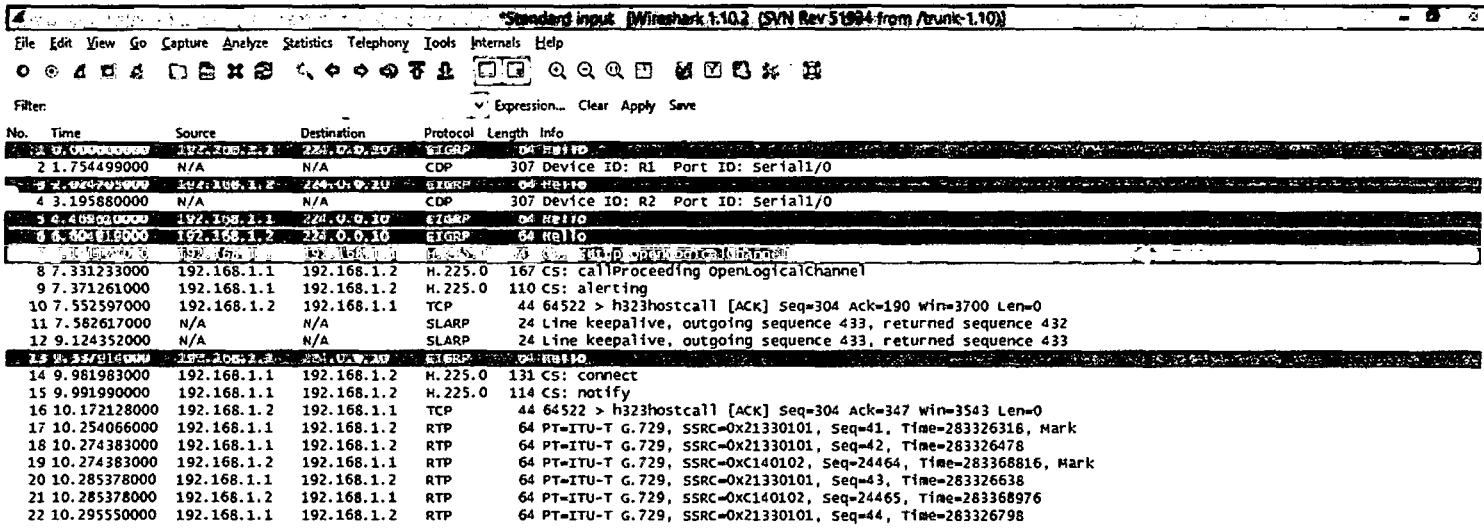


Fig. 4.9.14 Captura del paquete H.225.0 con Wireshark.

En esta imagen se puede analizar detalladamente el paquete H.225.0

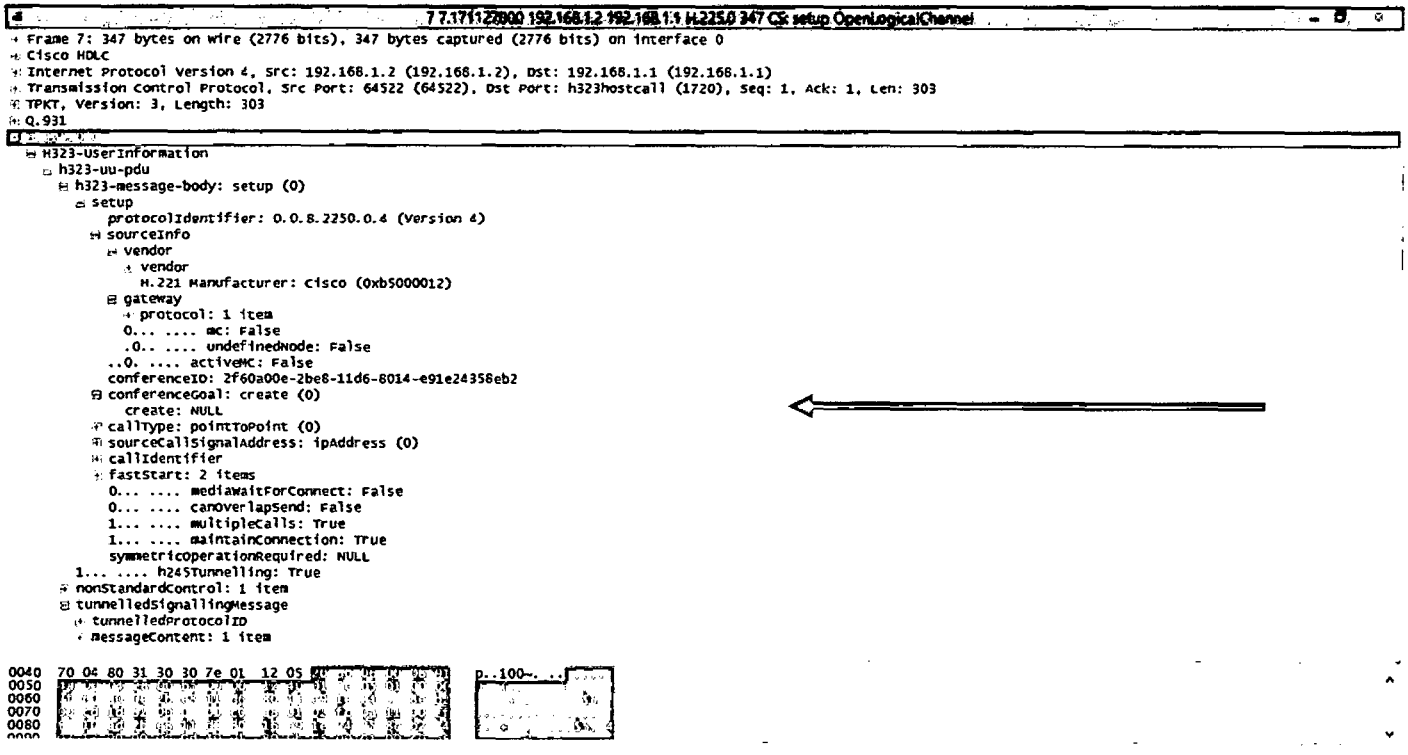


Fig. 4.9.15 Información detallada del paquete H.225.0.

- Captura de paquetes **Q.931**, fue diseñado por RDSI para establecimiento de llamada, mantenimiento y liberación de conexiones de red entre dos DTE

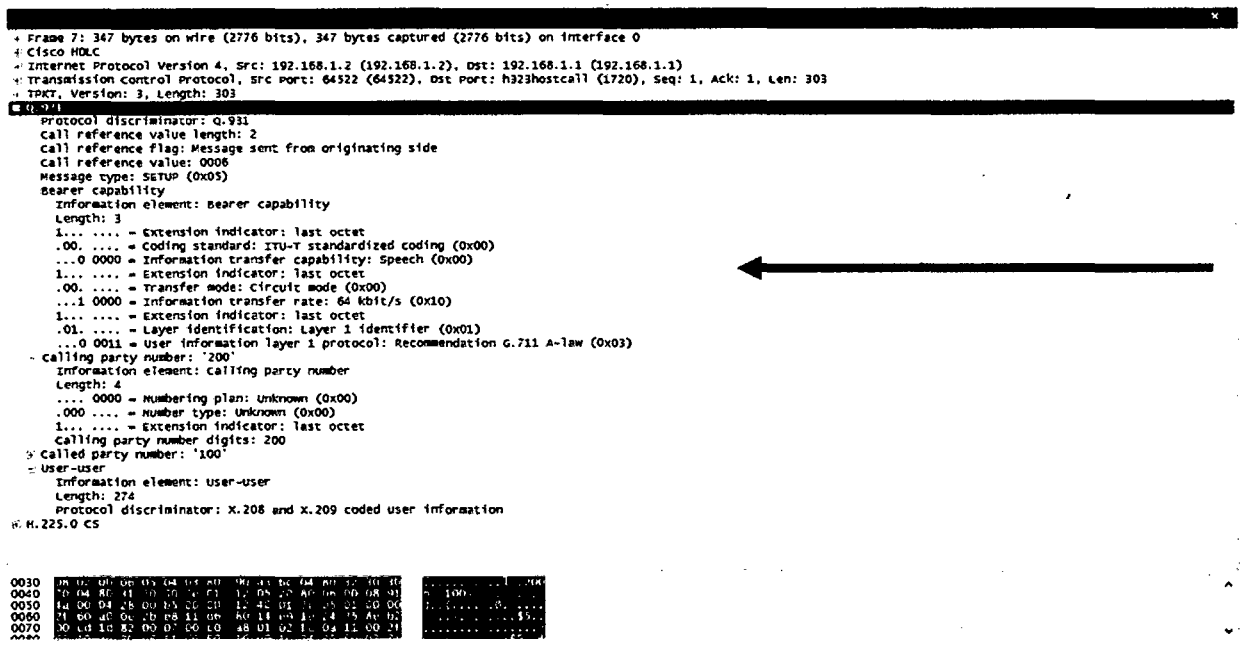


Fig. 4.9.16 Captura del paquete Q.931 con Wireshark.

PASO 2: Análisis de Jitter de una llamada y prueba de servicio de calidad (QoS)

Seleccionar un paquete RTP y hacer clic en **Telephony**, luego escoger **RTP** y finalmente **Show All Streams.**

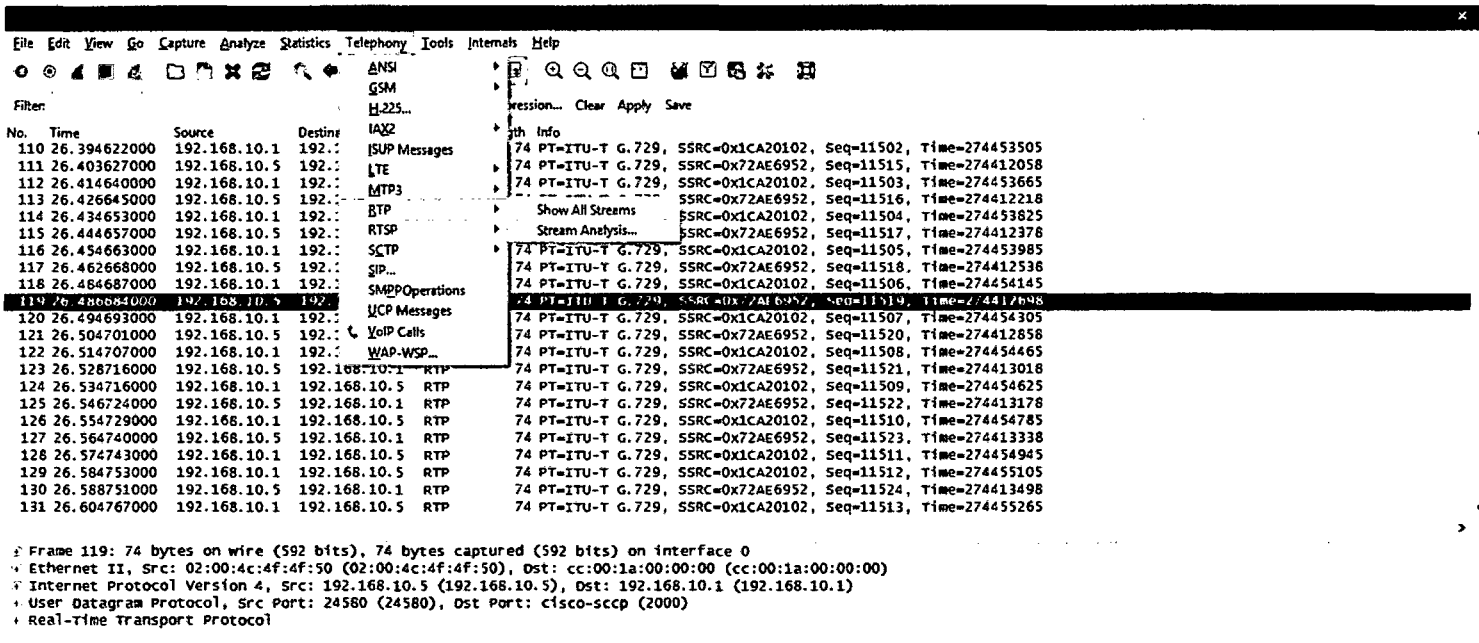


Fig. 4.9.17 Show All Streams.

En esta imagen se observa la llamada realizada, también datos adicionales como Jitter, numero de paquetes recibidos y perdidos, etc.

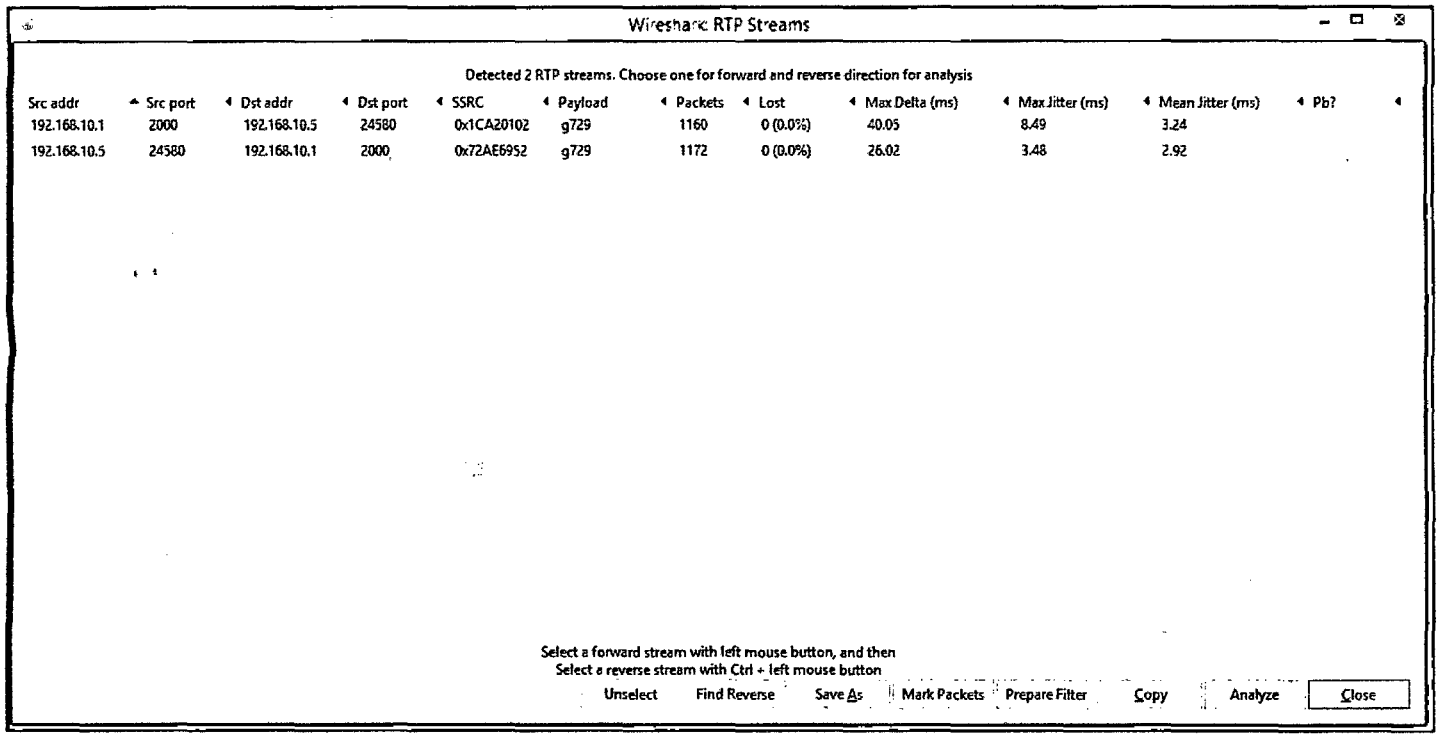


Fig. 4.9.18 Captura de tráfico de red con Wireshark.

Seleccionamos el primer ítem y damos clic en **Analyze.**

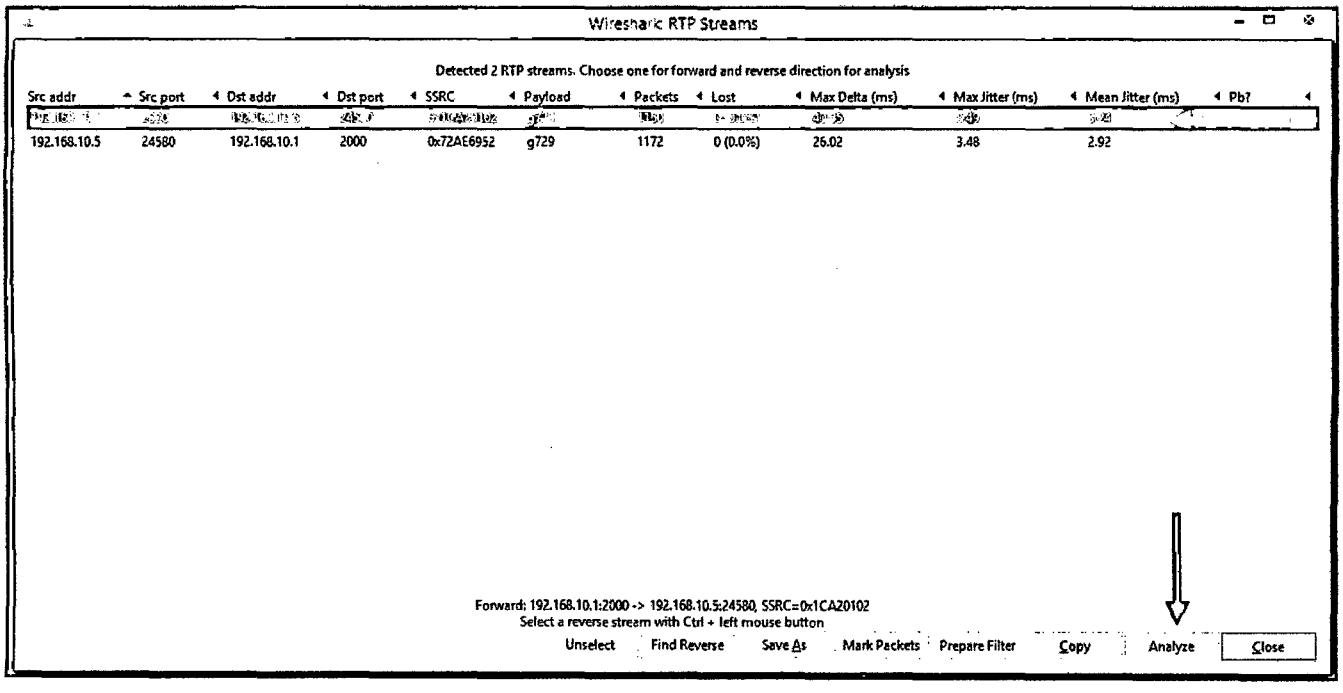


Fig. 4.9.19 Analyze

Nos mostrará la siguiente imagen, donde podemos observar el ancho de banda, el estado, etc. Seleccionamos el primer ítem y clic en **Graph**

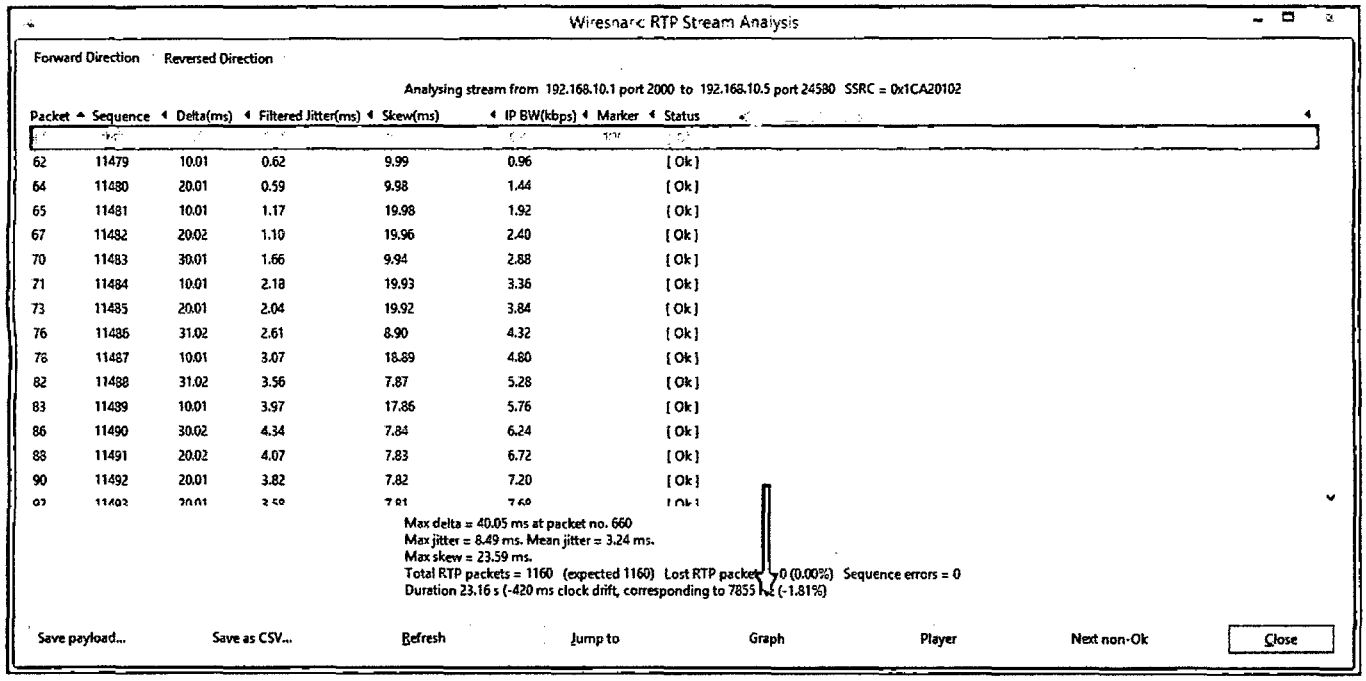


Fig. 4.9.20 Captura de tráfico de red con Wireshark.

Podemos observar la gráfica del Jitter de la llamada realizada.

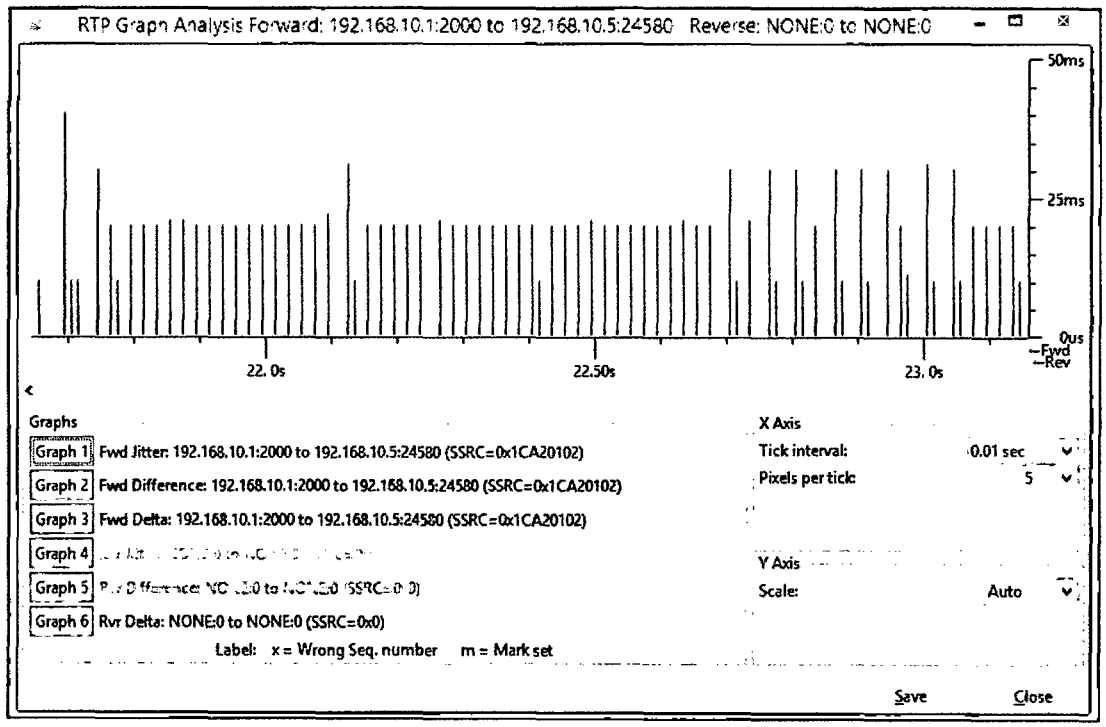


Fig. 4.9.21 Gráfica de Jitter.

También podemos escuchar el audio de la llamada, seleccionando el primer ítem y clic en **Player.**

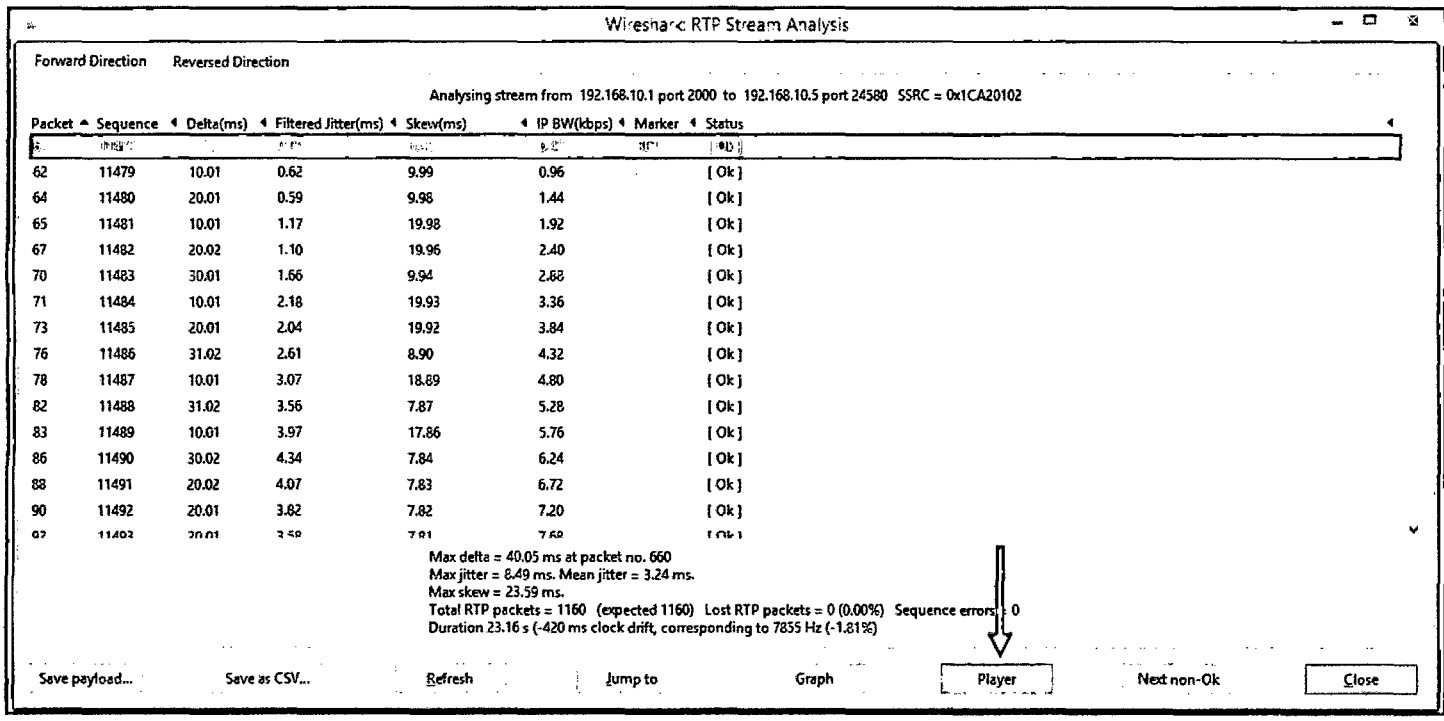


Fig. 4.9.22 Captura de tráfico de red con Wireshark.

Nos tratará la siguiente ventana, la cual tendrá un jitter buffer de 50 ms, clic en **Decode**

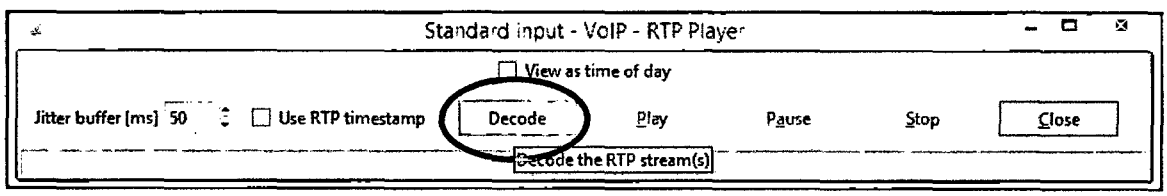


Fig. 4.9.23 Captura de tráfico de red con Wireshark.

Finalmente se podrá escuchar el audio de la llamada realizada.

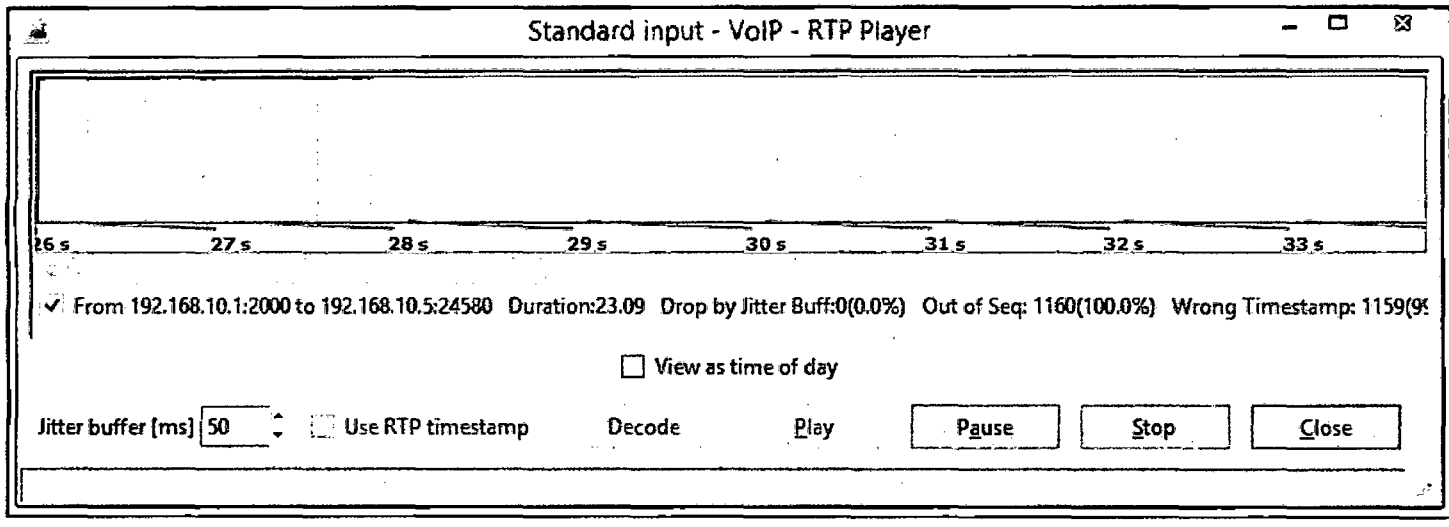


Fig. 4.9.24 Reproducción de audio.

LABORATORIO Nº 4.10: CONFIGURACIÓN BÁSICA DE PPP

REVISIÓN TEÓRICA: Para la realización de esta práctica se deberá revisar conceptos de fundamentales de la comunicación serial punto a punto (PPP).

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red según el diagrama de topología.
- Realizar tareas de configuración básica en los routers.
- Configurar y activar interfaces.
- Configurar el enrutamiento OSPF en todos los routers.
- Configurar la encapsulación PPP en todas las interfaces seriales.
- Configurar la autenticación CHAP y PAP de PPP.
- Aprender acerca de los comandos **debug ppp negotiation y debug ppp authentication**.
- Probar conectividad en la red y funcionamiento de PPP.
- Aprender cómo cambiar la encapsulación en las interfaces seriales de PPP a HDLC.

ESCENARIO:

En este laboratorio, se aprenderá a configurar la encapsulación PPP, la autenticación PPP PAP y la autenticación PPP CHAP en enlaces seriales a través de la red que se muestra en el diagrama de topología. Utilice la dirección 172.16.10.0/24 para obtener el direccionamiento IP usando VLSM, para los enlaces WAN entre routers, para el enlace entre el R2 y el ISP utilice la dirección IP 200.200.200.0/30 y para los enlaces LAN utilice 172.16.20.0/24 y 172.16.30.0/24 teniendo en cuenta los requisitos de las redes.

LAN R4: 200 host.

LAN R5: 124 host.

DIAGRAMA DE TOPOLOGIA:

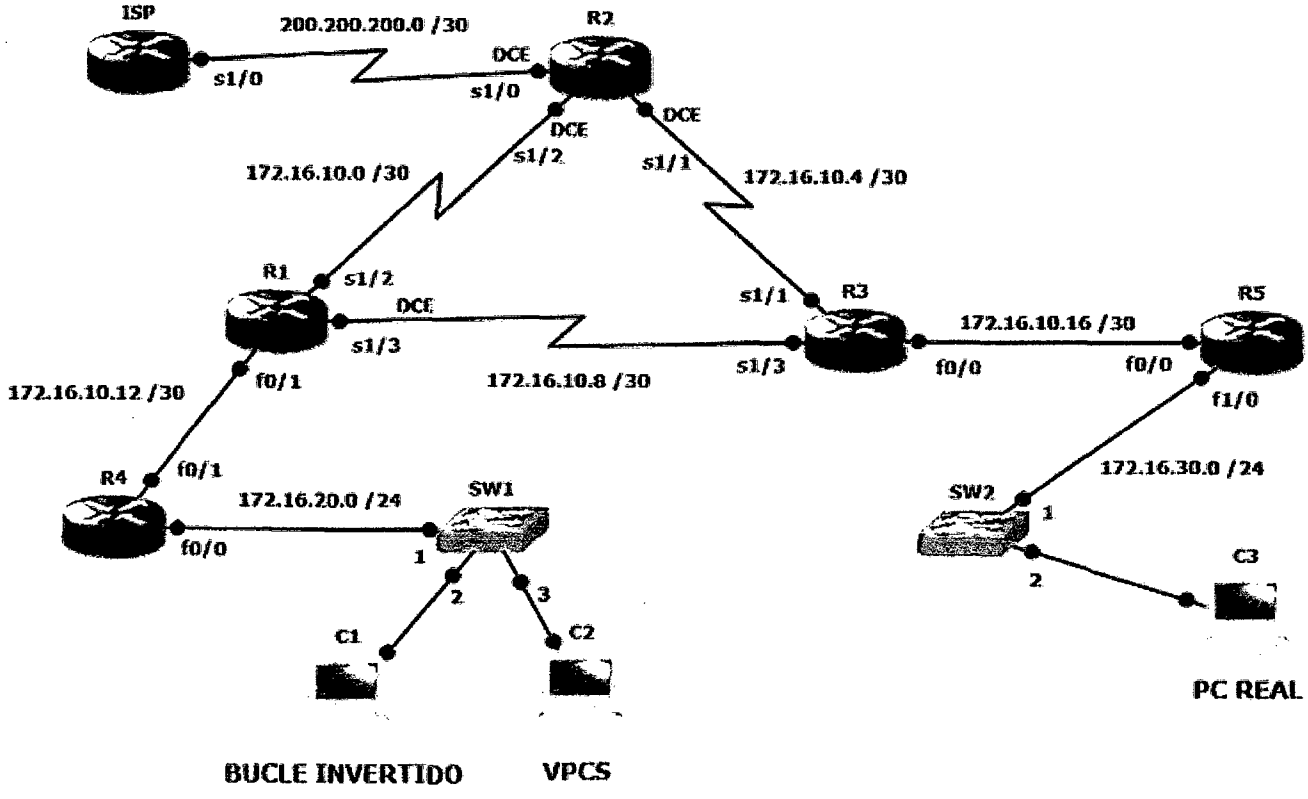


Fig. 4.10.1 Diagrama de topología en GNS3.

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN:

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	f0/1	172.16.10.13	255.255.255.252	No aplicable
	s1/2	172.16.10.2	255.255.255.252	No aplicable
	s1/3	172.16.10.9	255.255.255.252	No aplicable
R2	s1/0	200.200.200.1	255.255.255.252	No aplicable
	s1/1	172.16.10.5	255.255.255.252	No aplicable
	s1/2	172.16.10.1	255.255.255.252	No aplicable
R3	s1/1	172.16.10.6	255.255.255.252	No aplicable
	s1/3	172.16.10.10	255.255.255.252	No aplicable
	f1/0	172.16.10.17	255.255.255.252	No aplicable
R4	f0/0	172.16.20.1	255.255.255.0	No aplicable
	f0/1	172.16.10.14	255.255.255.0	No aplicable
R5	f1/0	172.16.30.1	255.255.255.0	No aplicable
	f0/0	172.16.10.18	255.255.255.252	No aplicable
ISP	S1/0	200.200.200.2	255.255.255.252	No aplicable
C1	BUCLE INVERTIDO	172.16.20.2	255.255.255.0	172.16.20.1
C2	VPCS	172.16.20.3	255.255.255.0	172.16.20.1
PC REAL	NIC	172.16.30.2	255.255.255.0	172.16.30.1

Tabla 4.10.1 Direccionamiento IP para las Redes

TAREA 1: MONTAR LA RED EN GNS3

Montar y conectar la red igual a la del Diagrama de topología.

TAREA 2: REALIZAR LA CONFIGURACIÓN BÁSICA DEL ROUTER

Configure los routers R1, R2, R3, R4, y R5 de acuerdo a las siguientes instrucciones desde el modo de configuración:

PASO 1: Configure el nombre de host del router.

PASO 2: Deshabilite la búsqueda DNS.

PASO 3: Configure una contraseña de Modo EXEC.

PASO 4: Configure un mensaje del día.

PASO 5: Configure una contraseña para las conexiones de la consola.

PASO 6: Configure una contraseña para las conexiones de vty.

PASO 7: Configure el registro de datos sincrónico.

PASO 8: Guardar la configuración en cada router.

TAREA 3: CONFIGURAR Y ACTIVAR LAS DIRECCIONES SERIAL Y FASTETHERNET

PASO 1: Configurar las interfaces de los routers.

Configure las interfaces de los routers R1, R2, R3, R4, R5 e ISP con las direcciones IP de la tabla de direccionamiento que se encuentra al comienzo de esta práctica de laboratorio. Asegúrese de incluir la frecuencia de reloj en las interfaces DCE seriales de los routers R2 y R1, en R3 son interfaces DTE.

R2:

Configuración de las interfaces serial DCE:

R2(config)#**interface serial 1/0**

R2(config-if)#**ip address 200.200.200.1 255.255.255.252**

R2(config-if)#**description conexión a ISP**

R2(config-if)#**clock rate 64000**

R2(config-if)#**no shutdown**

R2(config-if)#**exit**

R2(config)#**interface serial 1/1**

R2(config-if)#**ip address 172.16.10.2 255.255.255.252**

R2(config-if)#**description conexión a R3**

R2(config-if)#**clock rate 64000**

R2(config-if)#**no shutdown**

R2(config-if)#**exit**

R2(config)#**interface serial 1/2**

R2(config-if)#**ip address 172.16.10.1 255.255.255.252**

R2(config-if)#**description conexión a R1**

R2(config-if)#**clock rate 64000**

R2(config-if)#**no shutdown**

R2(config-if)#**exit**

R3:

Configuración de la interface serial DTE:

R3(config)#**interface serial 1/2**

R3(config-if)#**ip address 172.16.10.2 255.255.255.252**

R3(config-if)#**description conexión a R2**

R3(config-if)#**no shutdown**

R3(config-if)#**exit**

NOTA: Configurar las interfaces de los demás routers según corresponda.

PASO 2: Configurar las interfaces Loopback

En el router ISP configure las 3 interfaces loopback:

Loopback 1: 200.200.200.100 /32

Loopback 2: 200.200.200.200 /32

Loopback 3: 200.200.200.400 /32

ISP:

ISP(config)#**interface loopback 1**

ISP(config)# **ip address 200.200.200.100 255.255.255.255**

ISP(config)# **exit**

PASO 3: Guardar la configuración.

Guarde la configuración establecida de todos router con el comando **copy running-config startup-config.**

TAREA 4: CONFIGURAR EL PROTOCOLO OSPF

PASO 1: Configure una ruta estática por defecto en el router R2 para alcanzar las direcciones loopback del router ISP.

R2(config)#**ip route 0.0.0.0 0.0.0.0 s1/0**

PASO 2: Configure el protocolo de enrutamiento OSPF en todos los routers de la red para la conectividad.

R2(config)#**router ospf 100**

R2(config-router)#**network 172.16.10.0 0.0.0.3 area 0**

R2(config-router)#**network 172.16.10.4 0.0.0.3 area 0**

R2(config-router)#**default-information originate**

R2(config-router)#**exit**

R5(config)#**router ospf 100**

R5(config-router)#**network 172.16.10.16 0.0.0.3 area 0**

R5(config-router)# **network 172.16.30.0 0.0.0.255 area 0**

R5(config-router)#**passive-interface fastethernet 1/0**

R5(config-router)#**exit**

NOTA: Configurar el protocolo OSPF de la misma manera en los demás routers.

TAREA 5: CONFIGURACIÓN DE LA ENCAPSULACIÓN Y AUTENTICACIÓN PPP PAP Y PPP CHAP EN LAS INTERFACES SERIALES

Configuraremos el protocolo PPP PAP en las interfaces seriales que une R1 y R2, R2 y R3, R3 y R1, y el protocolo PPP CHAP en la interface serial que une el router ISP y R2. Para la configuración de la encapsulación y autenticación de PPP PAP y PPP CHAP en las interfaces seriales de los routers se debe seguir los siguientes pasos:

PASO 1: Comprobaremos que cada router tiene un nombre de host asignado, ya que se utilizará como nombre de usuario en la autenticación.

Router(config)#**hostmane R1**

PASO 2: Configuraremos en cada router el nombre de usuario y contraseña del router remoto, mediante el comando de configuración global **username [nombre] password [contraseña],** la contraseña debe ser la misma en ambos routers. Introduzca el comando de configuración global **service password-encryption** para proteger la contraseña configurada.

R1(config)#**username R2 password unprgpap**

R1(config)# **service password-encryption**

PASO 3: Habilitar el encapsulado PPP, para la configuración del encapsulado PPP ingresamos a la interface serial a utilizar, es opcional desactivar o no la interface.

R1(config)#**interface serial 1/2**

R1(config-if)#**shutdown**

R1(config-if)#**encapsulation ppp**

PASO 4: Configurar el protocolo de autenticación (PAP o CHAP) que deseamos utilizar mediante el siguiente comando de configuración de interfaz, tenemos que seguir dentro de la interface serial para la configuración de la autenticación, en este caso utilizamos la autenticación PAP.

R1(config-if)#**ppp authentication PAP**

R1(config-if)#**ppp pap sent-username R1 password unprgpap**

R1(config-if)#**no shutdown**

R1(config-if)#**exit**

PASO 5: Configuración de R2, la configuración de PPP PAP o PPP CAHP debe realizarse en ambos routers, en ambas interfaces seriales que los conecta, anteriormente mostramos la configuración de R1 ahora configuraremos R2:

Router(config)#**hostmane R2**

R2(config)#**username R1 password unprgpap**

R2(config)# **service password-encryption**

R2(config)#**interface serial 1/2**

R2(config-if)#**shutdown**

R2(config-if)#**encapsulation ppp**

R2(config-if)#**ppp authentication pap**

R2(config-if)#**ppp pap sent-username R2 password unprgpap**

R2(config-if)#**no shutdown**

R2(config-if)#**exit**

Configuración de PPP PAP en las interfaces seriales de R1 y R3:

R1:

R1(config)#**username R3 password unprgpap**

R1(config)#**interface serial 1/3**

R1(config-if)#**shutdown**

R1(config-if)#**encapsulation ppp**

R1(config-if)#**ppp authentication PAP**

R1(config-if)#**ppp pap sent-username R1 password unprgpap**

R1(config-if)#**no shutdown**

R1(config-if)#**exit**

R3:

Router(config)#**hostname R3**

R3(config)#**username R3 password unprgpap**

R3(config)#**service password-encryption**

R3(config)#**interface serial 1/3**

R3(config-if)#**shutdown**

R3(config-if)#**encapsulation ppp**

R3(config-if)#**ppp authentication pap**

R3(config-if)#**ppp pap sent-username R3 password unprgpap**

R3(config-if)#**no shutdown**

R3(config-if)#**exit**

NOTA: Seguir los mismos pasos para la configuración del enlace que hace falta el de R2 y R3.

Configuración de PPP CHAP en la interface serial del router ISP y R2:

R2:

Router(config)#**hostmane R2**

R2(config)#**username ISP password unprgchap**

R2(config)#**interface serial 1/0**

R2(config-if)#**shutdown**

R2(config-if)#**encapsulation ppp**

R2(config-if)#**ppp authentication chap**

R2(config-if)#**no shutdown**

R2(config-if)#**exit**

ISP:

ISP(config)#**hostname ISP**

ISP(config)# **service password-encryption**

ISP(config)#**username R2 password unprgchap**

ISP(config)#**interface serial 1/0**

ISP(config-if)#**shutdown**

ISP(config-if)#**encapsulation ppp**

ISP(config-if)#**ppp authentication chap**

ISP(config-if)#**no shutdown**

ISP(config-if)#**exit**

Para restablecer las interfaces seriales de los routers a su encapsulación HDLC por defecto se puede hacer configurándolas de dos formas:

FORMA 1:

R2:

R2(config)#**interface serial 1/0**

R2(config-if)#**encapsulation hdlc**

R2(config-if)#**shutdown**

R2(config-if)# **no shutdown**

R2(config-if)#**exit**

FORMA 2:

R2:

R2(config)#**interface serial 1/0**

R2(config-if)#**no encapsulation ppp**

R2(config-if)#**shutdown**

R2(config-if)# **no shutdown**

R2(config-if)#**exit**

NOTA: Realizar la misma configuración en el otro extremo de la interface serial (en este caso en el router ISP) para que haya concordancia entre sus tipos de encapsulación.

TAREA 6: CONFIGURAR LOS EQUIPOS DE HOST.

Configurar las direcciones IP y gateways por defecto como se indican en la tabla de direccionamiento de las interfaces Ethernet de C1, C2 (VPCS) y PC REAL.

TAREA 7: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

PASO 1: Verificar el direccionamiento IP y las interfaces.

R1**#show ip interface brief**

```
R1#
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM  administratively down down
FastEthernet0/1            172.16.10.13    YES NVRAM  up                    up
Serial1/0                  unassigned      YES NVRAM  administratively down down
Serial1/1                  unassigned      YES NVRAM  administratively down down
Serial1/2                  172.16.10.2     YES NVRAM  up                    up
Serial1/3                  172.16.10.9     YES NVRAM  up                    up
R1#
```

Fig. 4.10.2 Tabla ip de interface brief de R1.

NOTA: Verificar que las interfaces de los demás routers tengan la adecuada dirección IP y estén activas.

PASO 2: Verificar la configuración de los router. Use los comandos **show ip route** para verificar el contenido de la tabla de enrutamiento.

R2**#show ip route**

```
R1#
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.16.10.1 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.16.30.0/24 [110/66] via 172.16.10.10, 00:11:33, Serial1/3
O       172.16.10.16/30 [110/65] via 172.16.10.10, 00:11:33, Serial1/3
O       172.16.20.0/24 [110/2] via 172.16.10.14, 00:11:33, FastEthernet0/1
O       172.16.10.4/30 [110/128] via 172.16.10.10, 00:11:33, Serial1/3
                       [110/128] via 172.16.10.1, 00:11:33, Serial1/2
C       172.16.10.0/30 is directly connected, Serial1/2
C       172.16.10.1/32 is directly connected, Serial1/2
C       172.16.10.12/30 is directly connected, FastEthernet0/1
C       172.16.10.10/32 is directly connected, Serial1/3
C       172.16.10.8/30 is directly connected, Serial1/3
O*E2 0.0.0.0/0 [110/1] via 172.16.10.1, 00:11:35, Serial1/2
R1#
```

Fig. 4.10.3 Tabla de enrutamiento de R1.

NOTA: Verificar de igual manera la tabla de enrutamiento de los demás routers.

PASO 3: Una vez que hemos configurado PPP PAP o PPP CHAP, verificaremos la configuración de PPP en las interfaces configurada con el comando show interface, como se muestra a continuación.

R2#**show interface serial 1/0**

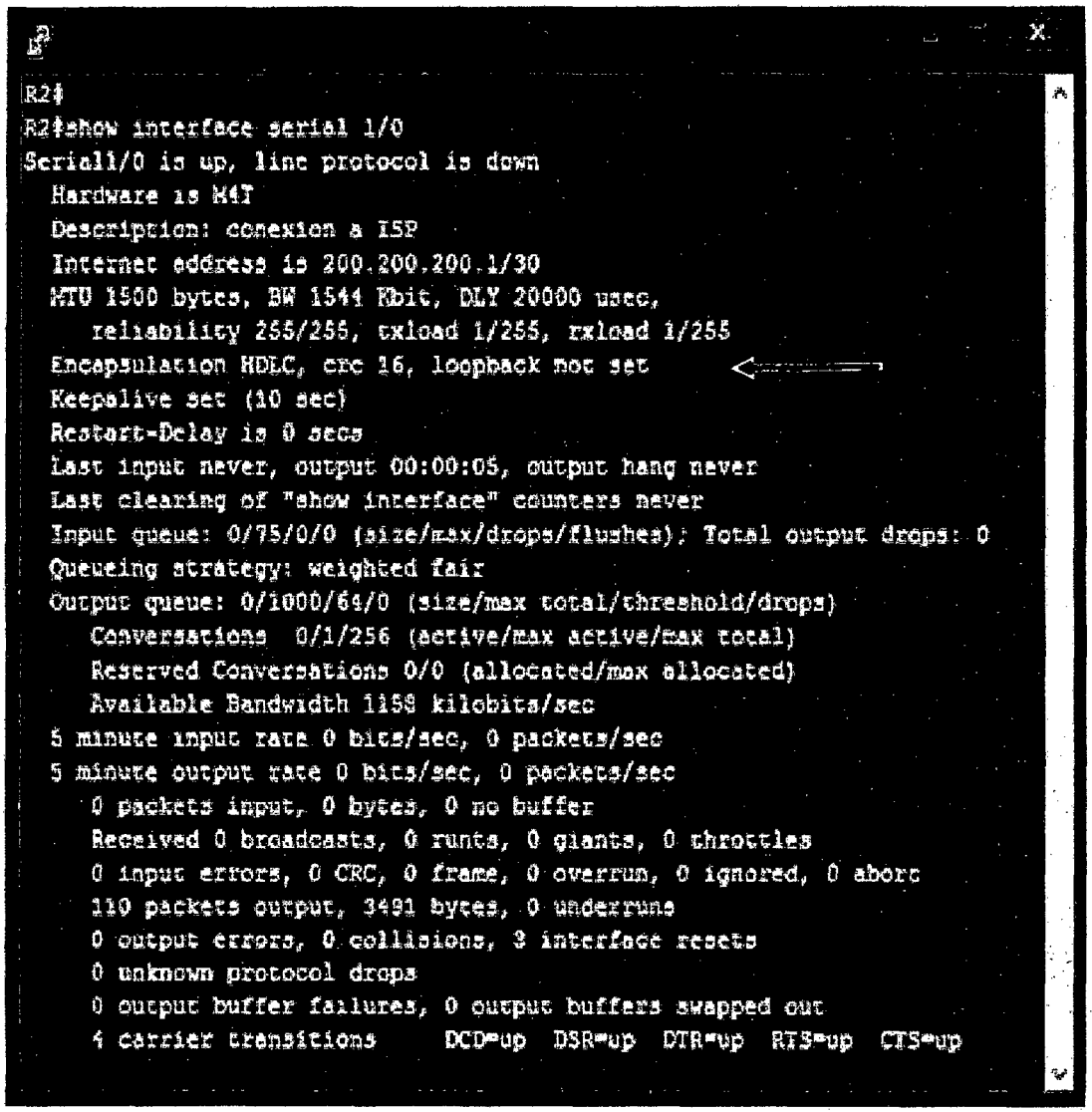


Fig. 4.10.4 Interface serial de R2 antes de ser configurada con la encapsulación PPP (HDLC).

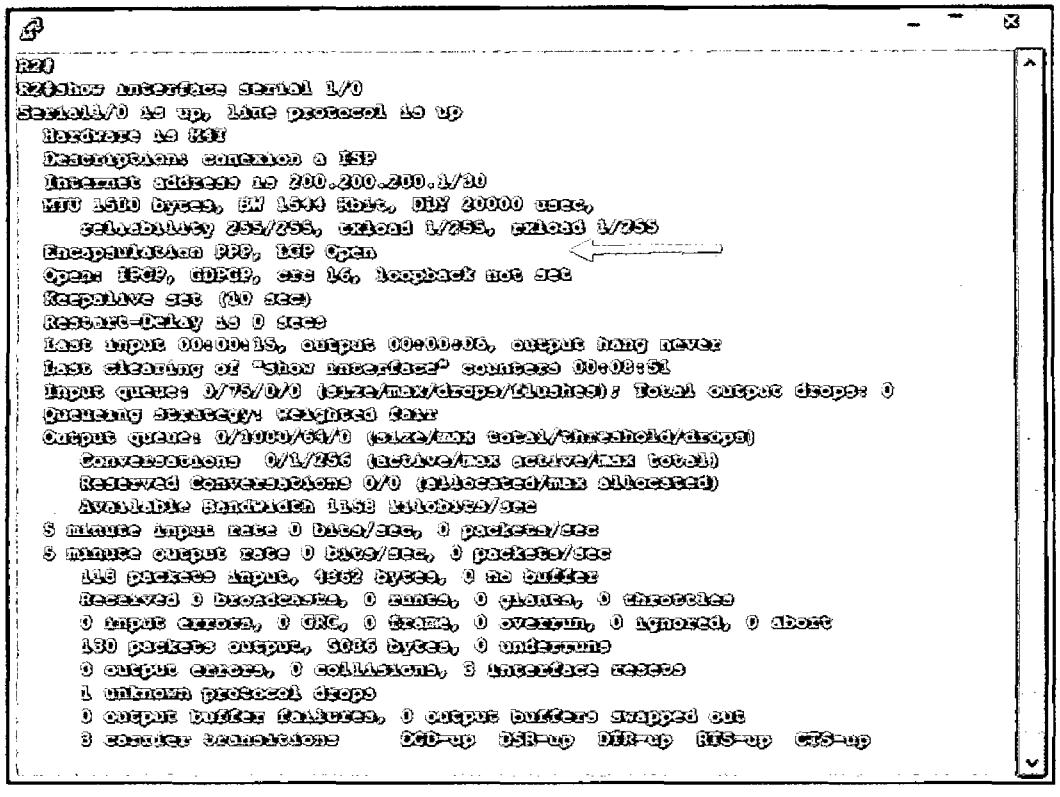


Fig. 4.10.5 Interface serial de R2 configurada con la encapsulación PPP.

ISP#show interface serial 1/0

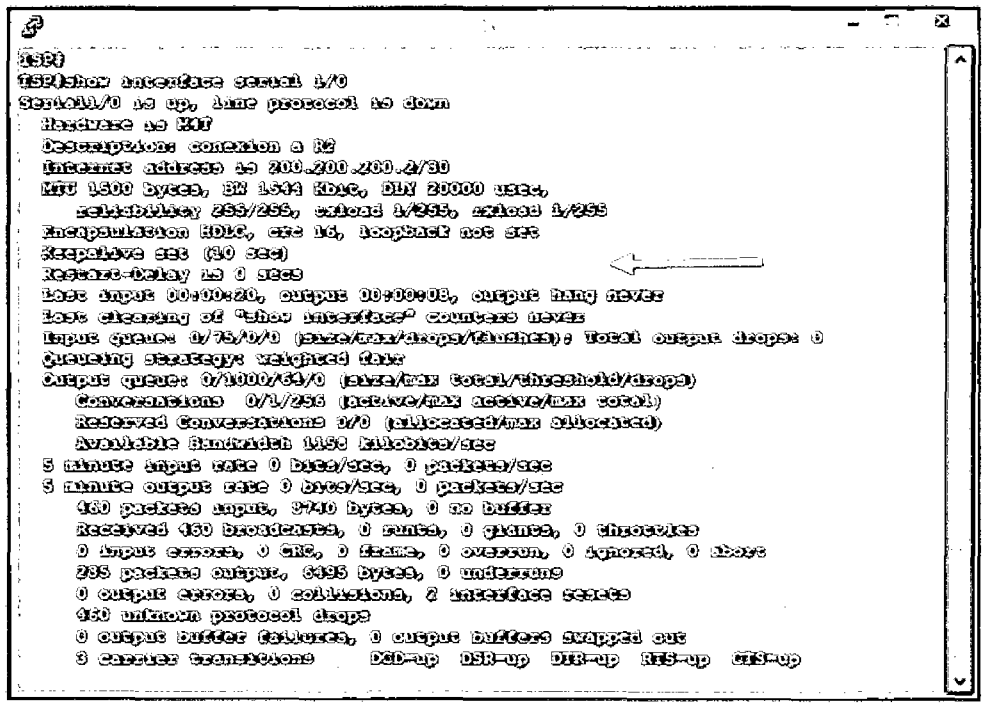


Fig. 4.10.6 Interface serial de ISP antes de ser configurada con la encapsulación PPP (HDLC).

Fig. 4.10.7 Interface serial de ISP configurada con la encapsulación PPP.

NOTA: Verificar que todas las interfaces donde hemos configurado PPP hayan cambiado de encapsulación de HDLC a PPP.

PASO 4: Comandos debug de PPP.

El comando **debug ppp authentication** nos mostrara el proceso de autenticación de PAP o CHAP. Si es que la encapsulacion PPP y la autención están configurados correctamente en los routers, así como los nombres de usuario con sus respectivas contraseñas.

El comando **debug ppp negotiation** nos muestra los procesos de negociacion de PPP.

El proceso de verificación de la autenticación de PAP se realiza con el comando **debug ppp authentication,** el cuál debe ser configurado en ambos routers en este caso en R1 y R2, luego se ingresa a la interface donde ha sido configurado PAP y se le desactiva y activa como indica a continuación:

R1# **debug ppp authentication**

R1#**configure terminal**

R1(config)#**interface serial 1/2**

R1(config)#**shutdown**

R1(config)#**no shutdown**

```
R1(config)#
R1(config)#int serial 1/2
R1(config-if)#no shutdow
R1(config-if)#
*Mar  1 02:07:58.155: %LINK-3-UPDOWN: Interface Serial1/2, changed state to up
*Mar  1 02:07:58.163: Se1/2 PPP: Using default call direction
*Mar  1 02:07:58.167: Se1/2 PPP: Treating connection as a dedicated line
*Mar  1 02:07:58.171: Se1/2 PPP: Session handle[3F000009] Session id[9]
*Mar  1 02:07:58.171: Se1/2 PPP: Authorization required
*Mar  1 02:07:58.235: Se1/2 PAP: Using hostname from interface PAP
*Mar  1 02:07:58.239: Se1/2 PAP: Using password from interface PAP
*Mar  1 02:07:58.239: Se1/2 PAP: O AUTH-REQ id 2 len 16 from "R1"
*Mar  1 02:07:58.279: Se1/2 PAP: I AUTH-REQ id 2 len 16 from "R2"
*Mar  1 02:07:58.279: Se1/2 PAP: Authenticating peer R2
*Mar  1 02:07:58.283: Se1/2 PPP: Sent PAP LOGIN Request
*Mar  1 02:07:58.283: Se1/2 PPP: Received LOGIN Response PASS
*Mar  1 02:07:58.287: Se1/2 PPP: Sent LCP AUTHOR Request
*Mar  1 02:07:58.295: Se1/2 PPP: Sent IPCP AUTHOR Request
*Mar  1 02:07:58.307: Se1/2 LCP: Received AAA AUTHOR Response PASS
*Mar  1 02:07:58.315: Se1/2 IPCP: Received AAA AUTHOR Response PASS
*Mar  1 02:07:58.315: Se1/2 PAP: O AUTH-ACK id 2 len 5
*Mar  1 02:07:58.355: Se1/2 PAP: I AUTH-ACK id 2 len 5
*Mar  1 02:07:58.363: Se1/2 PPP: Sent CDPCP AUTHOR Request
*Mar  1 02:07:58.375: Se1/2 CDPCP: Received AAA AUTHOR Response PASS
*Mar  1 02:07:58.395: Se1/2 PPP: Sent IPCP AUTHOR Request
*Mar  1 02:07:58.711: %OSPF-5-ADJCHG: Process 100, Nbr 200.200.200.1 on Serial1/2 from
 LOADING to FULL, Loading Done
*Mar  1 02:07:59.359: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/2, chang
ed state to up
R1(config-if)#
```

Fig. 4.10.8 Verificando la autenticación de PAP en R1

R2# **debug ppp authentication**

```
R2#
R2#debug ppp authentication
PPP authentication debugging is on
R2#
*Mar  1 02:07:53.979: Se1/2 PPP: Authorization required
*Mar  1 02:07:54.043: Se1/2 PAP: Using hostname from interface PAP
*Mar  1 02:07:54.043: Se1/2 PAP: Using password from interface PAP
*Mar  1 02:07:54.047: Se1/2 PAP: O AUTH-REQ id 2 len 16 from "R2"
*Mar  1 02:07:54.083: Se1/2 PAP: I AUTH-REQ id 2 len 16 from "R1"
*Mar  1 02:07:54.083: Se1/2 PAP: Authenticating peer R1
*Mar  1 02:07:54.083: Se1/2 PPP: Sent PAP LOGIN Request
*Mar  1 02:07:54.083: Se1/2 PPP: Received LOGIN Response PASS
*Mar  1 02:07:54.091: Se1/2 PPP: Sent LCP AUTHOR Request
*Mar  1 02:07:54.095: Se1/2 PPP: Sent IPCP AUTHOR Request
*Mar  1 02:07:54.103: Se1/2 PAP: I AUTH-ACK id 2 len 5
*Mar  1 02:07:54.111: Se1/2 LCP: Received AAA AUTHOR Response PASS
*Mar  1 02:07:54.115: Se1/2 IPCP: Received AAA AUTHOR Response PASS
*Mar  1 02:07:54.119: Se1/2 PAP: O AUTH-ACK id 2 len 5
*Mar  1 02:07:54.127: Se1/2 PPP: Sent CDPCP AUTHOR Request
*Mar  1 02:07:54.143: Se1/2 CDPCP: Received AAA AUTHOR Response PASS
*Mar  1 02:07:54.155: Se1/2 PPP: Sent IPCP AUTHOR Request
*Mar  1 02:07:54.555: %OSPF-5-ADJCHG: Process 100, Nbr 172.16.10.13 on Serial1/2 from LOADING to
 Done
*Mar  1 02:07:55.119: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/2, changed state to
R2#
```

Fig. 4.10.9 Verificando la autenticación de PAP en R2

El proceso de verificación de la autenticación de CHAP se realiza de la misma forma que PAP con el comando **debug ppp authentication,** entrando a la interface serial desactivándola y activandola.

R2# **debug ppp authentication**

R2#**configure terminal**

R2(config)#**interface serial 1/0**

R2(config)#**shutdown**

R2(config)#**no shutdown**

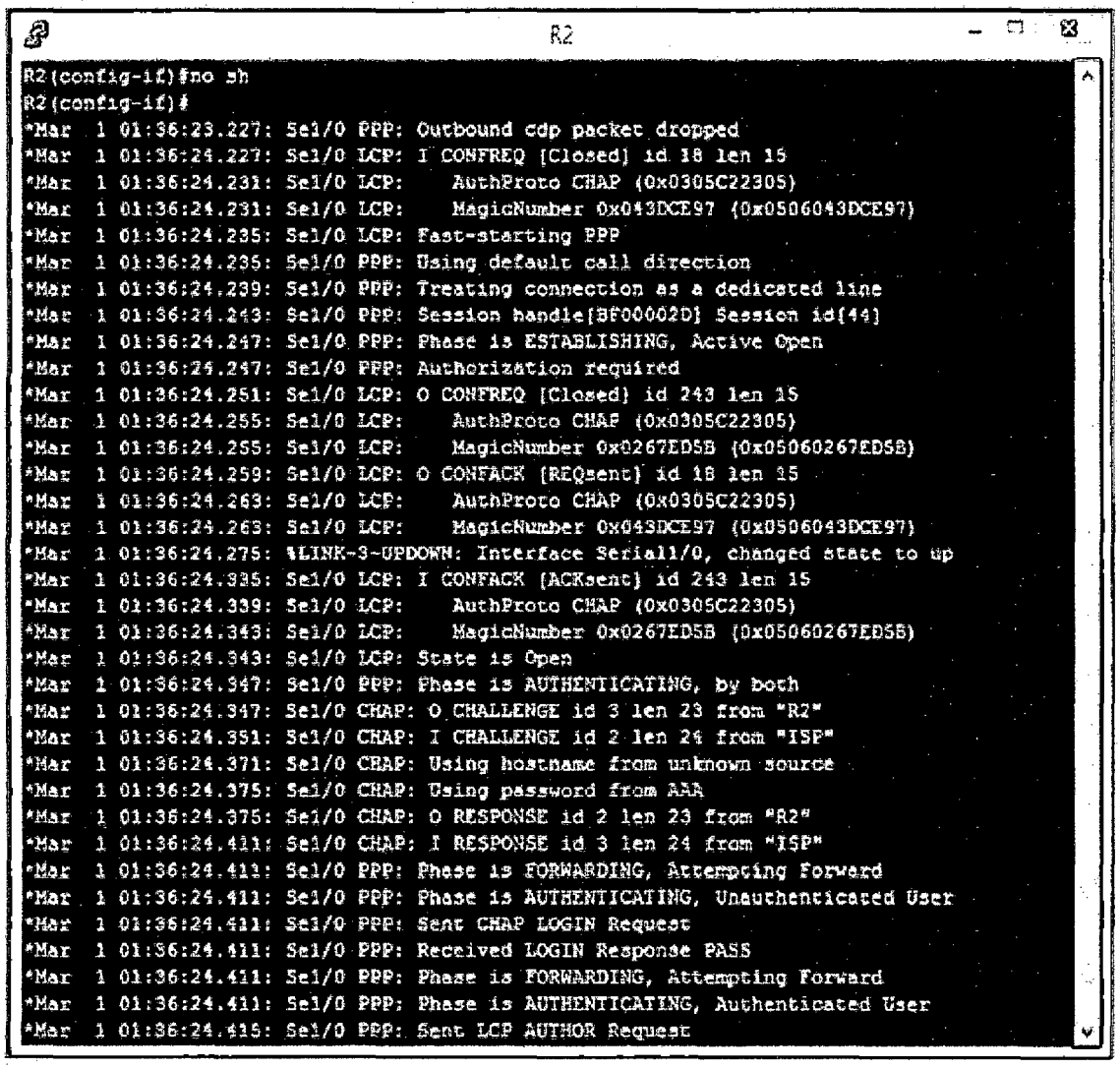


Fig. 4.10.10 Verificando la autenticación de CHAP en R2

ISP# **debug ppp authentication**

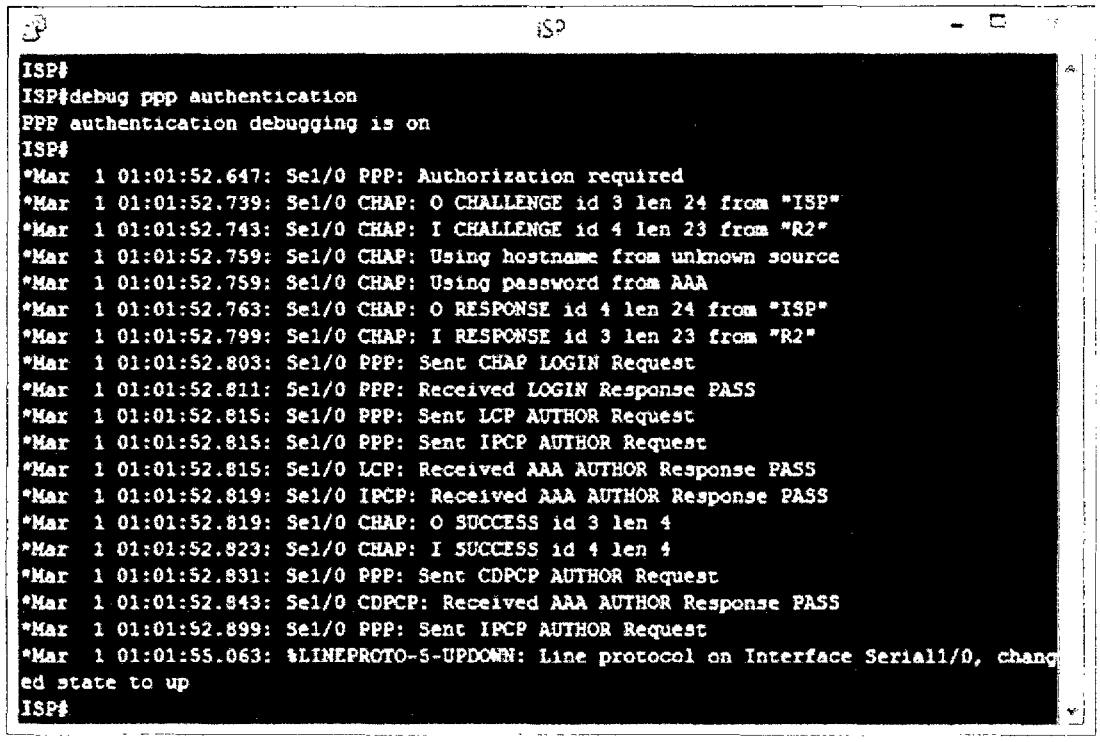


Fig. 4.10.11 Verificando la autenticación de CHAP en ISP

NOTA: Verificar la autenticidad de PAP en las demás interfaces seriales, para parar la autenticación colocamos el comando **undebug all**.

NOTA: El proceso de verificación de la negociación de PAP se realiza de la misma forma que el proceso de autenticación atreves del comando **debug ppp negotiation** el cual nos muestra los procesos de negociacion de PPP.

PASO 5: Verificar que hay conectividad completa en la red.

Use el comando **ping** para verificar la conectividad.

R2#**ping 172.16.20.1**

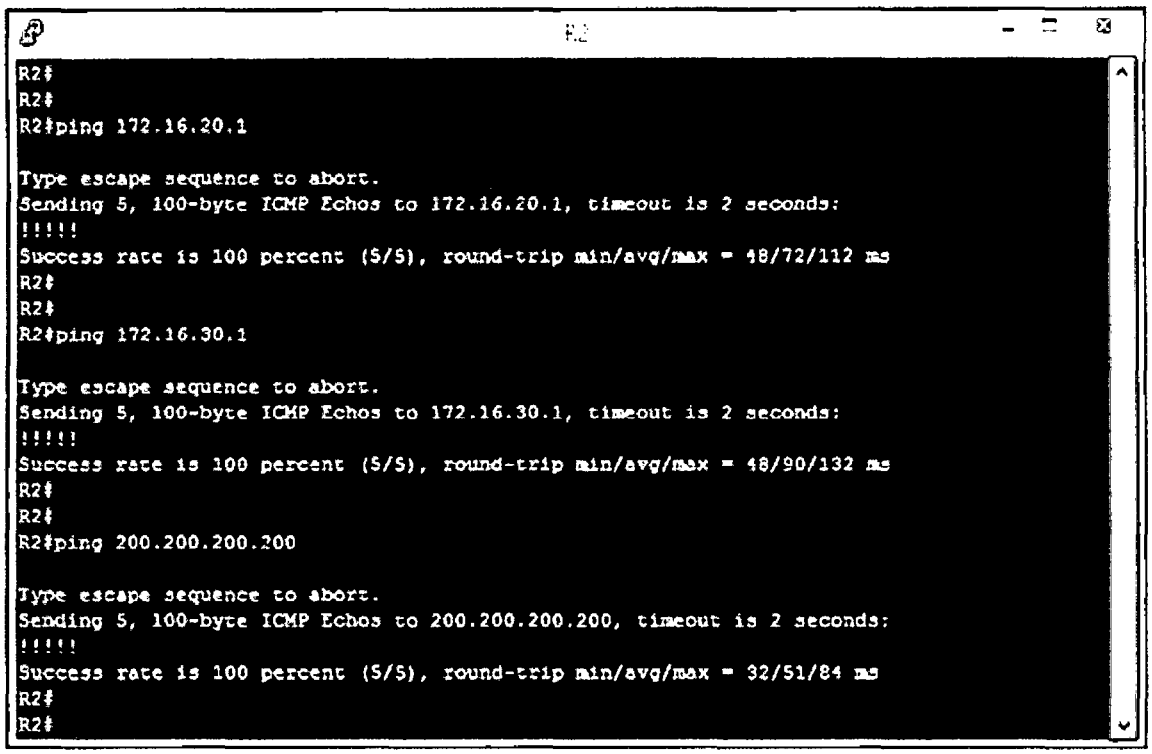


Fig. 4.10.12 Prueba de conectividad entre routers.

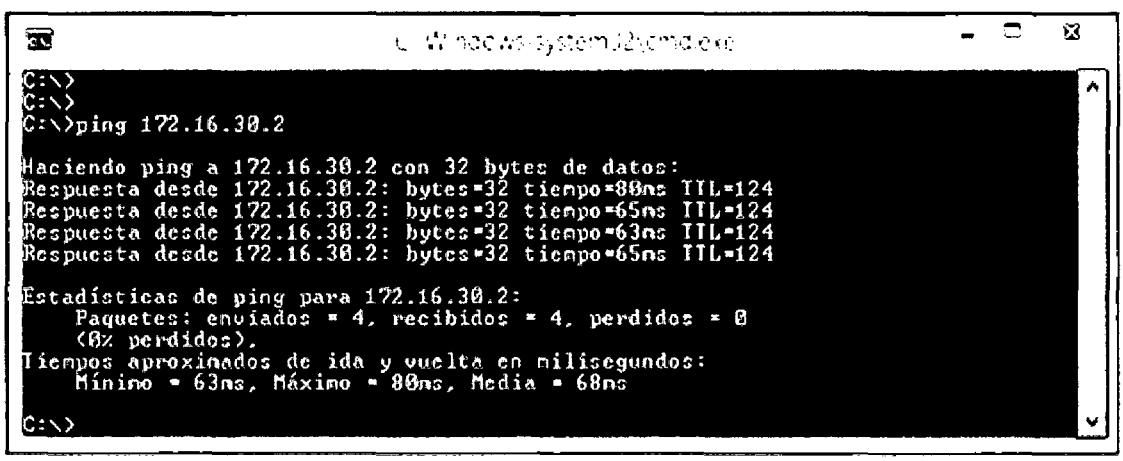


Fig. 4.10.13 Prueba de conectividad entre host desde C1 a PC real.

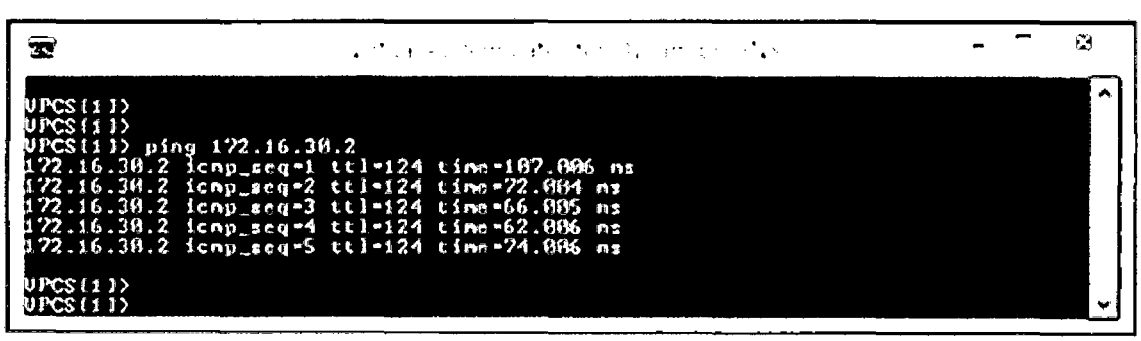


Fig. 4.10.14 Prueba de conectividad entre host desde C2 a PC real.

TAREA 8: ANALISIS DEL TRAFICO DE PAQUETES

PASO 1: Medición de la Latencia

Para la medición de la latencia se realizó 10 muestras sucesivas de 100 ping desde el C1 (Bucle invertido) hacia la PC REAL considerando un tamaño de trama de 64, 512 y 1518 bytes como se especifica en el RFC 2544.

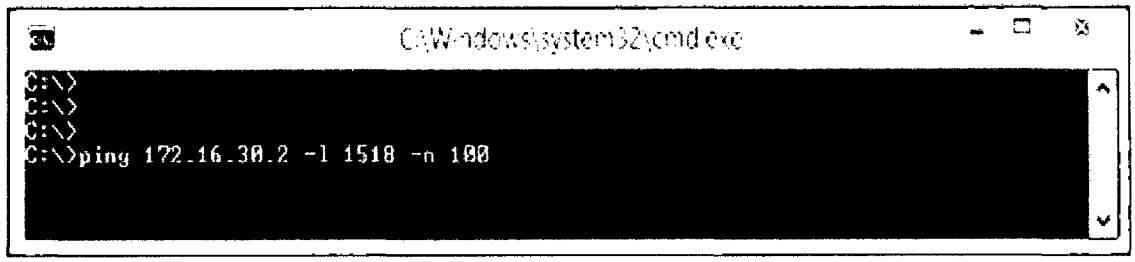


Fig. 4.10.15 Forma de medición de la latencia.

En la Figura 4.10.15 se puede observar el envío de 100 ping con una trama de 1518 hacia la dirección 172.16.30.2

En las Tablas posteriores se detallan los valores de la Latencia que se ha obtenido una vez realizadas todas las muestras.

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	**57**	**52**	**51**	**64**	**58**	**63**	**60**	**59**	**62**	**59**	**58.5**
Tiempo Máximo (ms)	**132**	**150**	**91**	**460**	**264**	**326**	**399**	**226**	**304**	**294**	**264.6**
Tiempo Promedio (ms)	**72**	**73**	**72**	**175**	**116**	**152**	**146**	**120**	**133**	**126**	**118.5**

Tabla 4.10.2 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**512**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	**59**	**62**	**61**	**59**	**58**	**59**	**66**	**56**	**61**	**58**	**59.9**
Tiempo Máximo (ms)	**110**	**535**	**331**	**345**	**310**	**336**	**354**	**310**	**301**	**264**	**319.6**
Tiempo Promedio (ms)	**72**	**205**	**134**	**148**	**116**	**173**	**114**	**136**	**171**	**117**	**138.6**

Tabla 4.10.3 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1518										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	62	69	62	66	65	80	72	58	66	64	66.4
Tiempo Máximo (ms)	586	340	257	278	425	275	368	291	406	455	368.1
Tiempo Promedio (ms)	167	186	151	142	115	162	131	138	164	132	148.8

Tabla 4.10.4 Comparación de datos obtenidos de las diferentes tramas.

LATENCIA			
Tamaño de Trama (bytes)	64	512	1518
Tiempo Mínimo (ms)	58.5	59.9	66.4
Tiempo Máximo (ms)	264.6	319.6	368.1
Tiempo Promedio (ms)	118.5	138.6	148.8

Tabla 4.10.5 Comparación de datos obtenidos de las diferentes tramas.

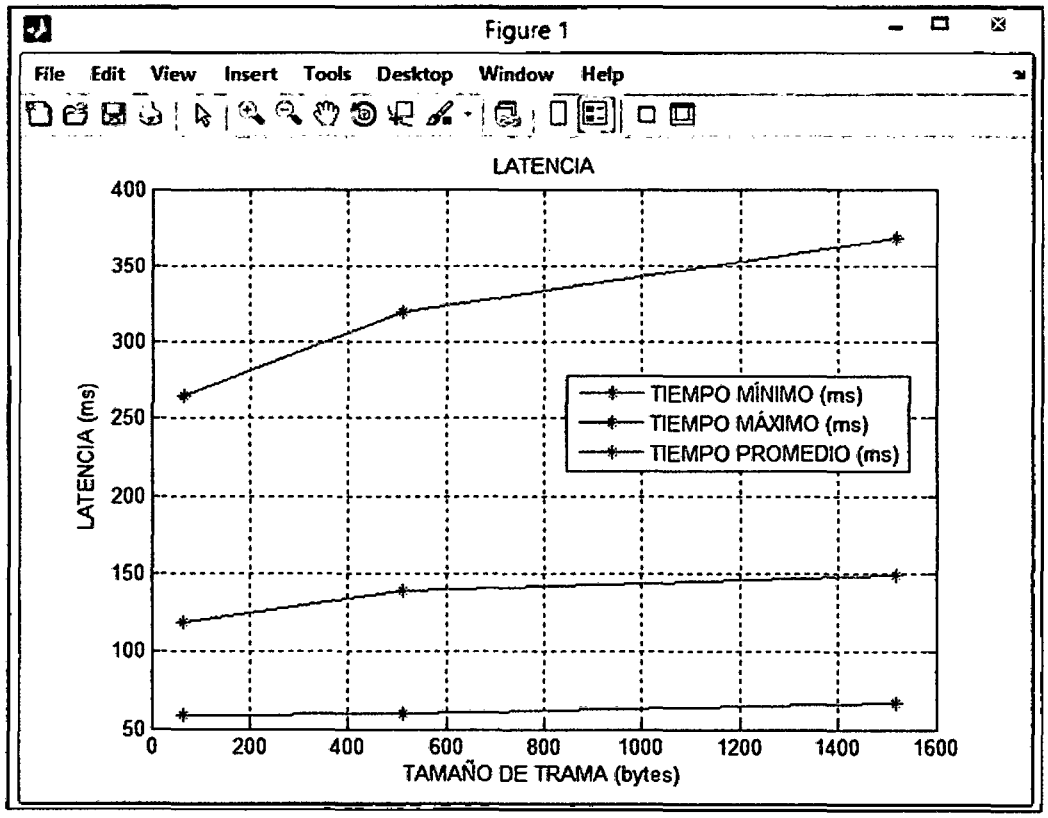


Fig. 4.10.16 Datos representados gráficamente de la variación de la latencia.

De acuerdo con los datos obtenidos, se puede observar claramente que los valores mínimo (color azul), máximo (color rojo) y promedio (color verde) de la latencia de la red se incrementan conforme se envía una trama de longitud mayor, en este caso con la trama de 1518 bytes se obtiene una latencia promedio de 148.8 ms a diferencia de una trama de 64 bytes con 118.5 ms.

PASO 2: Medición del Throughput

Para la medición del Throughput y Jitter se envió una cantidad de tramas a velocidades diferentes durante 20 segundos, hasta encontrar la máxima cantidad de tramas recibidas sin que se produzcan perdidas de las mismas en el router y PC REAL. Como se utilizó Jperf el cliente será el encargado de enviar los paquetes y el servidor los recibirá, indicando la cantidad de paquetes que llegaron correctamente considerando un tamaño del paquete UDP de 750, 1125, 1500 y 1470 (default) bytes, tal como se especifica en el RFC 768.

Configuración del Jperf como servidor para medir Throughput:

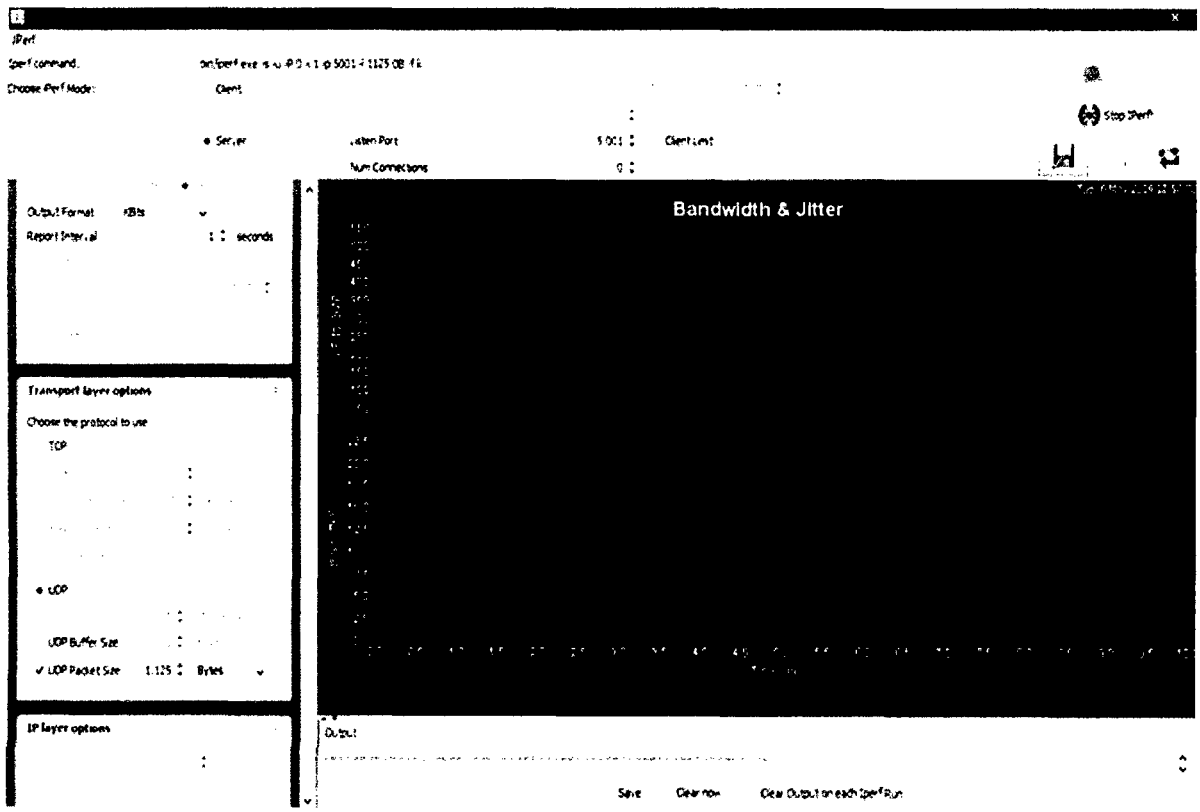


Fig. 4.10.17 Gráfica de Bandwidth y Jitter.

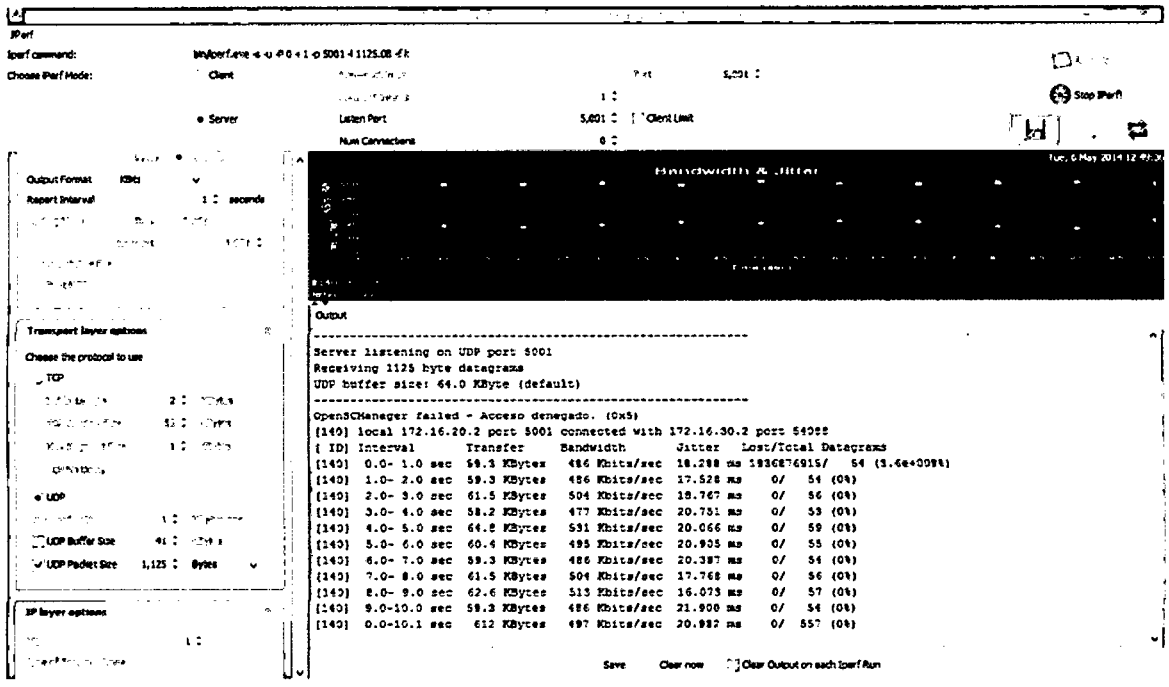


Fig. 4.10.18 Resultados al medir Throughput como servidor.

Configuración del Jperf como cliente para medir Throughput:

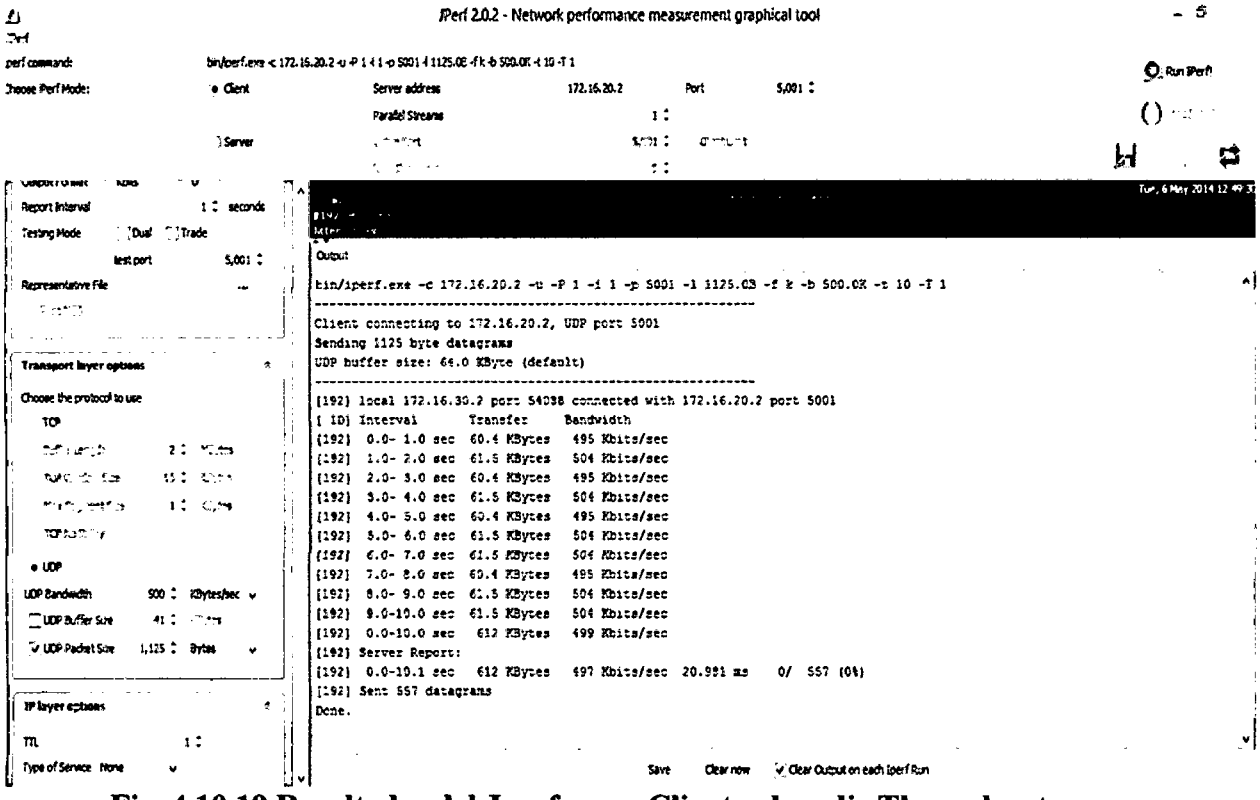


Fig. 4.10.19 Resultados del Jperf como Cliente al medir Throughput.

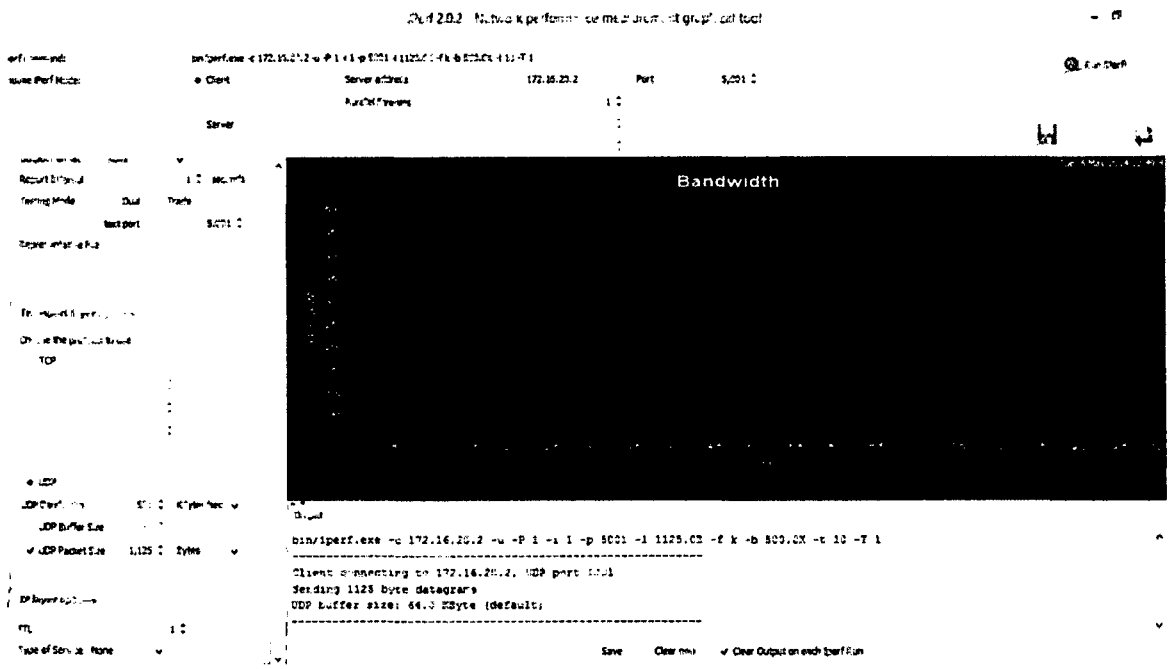


Fig. 4.10.20 Gráfica del Bandwidth.

En las siguientes Tablas se detalla los valores del Throughput obtenidos una vez realizada todas las muestras.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**0.5**	**0.5**	**0.5**
Velocidad de Rx (Mbps)	**0.5**	**0.497**	**0.496**
Tramas Transmitidas	**834**	**557**	**418**
Tramas Recibidas	**834**	**557**	**418**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**84**	**56**	**41**

Tabla 4.10.6 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**0.5**	**1**	**2**
Velocidad de Rx (Mbps)	**0.5**	**0.924**	**1.21**
Tramas Transmitidas	**426**	**851**	**1701**
Tramas Recibidas	**426**	**851**	**1613**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**88 (5.2%)**
Tramas Recibidas (pps)	**43**	**84**	**170**

Tabla 4.10.7 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

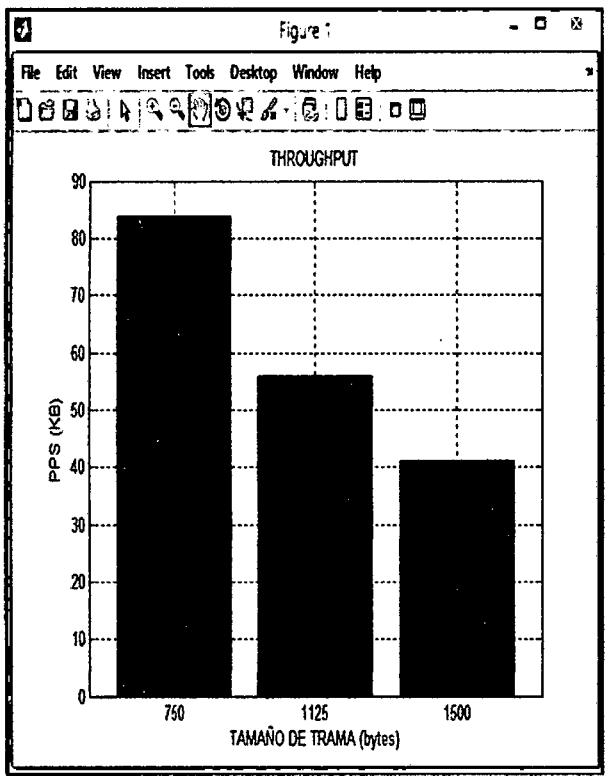


Fig. 4.10.21 PPS vs. Tamaño de Trama.

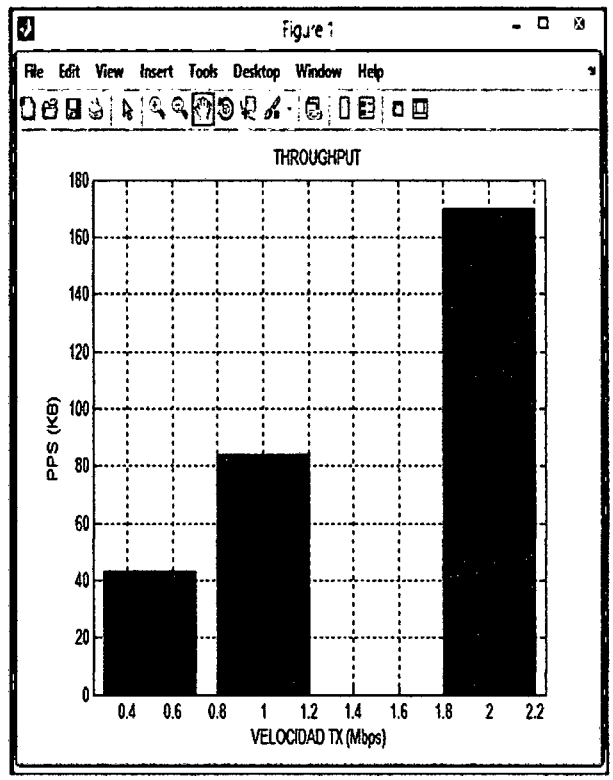


Fig. 4.10.22 PPS vs. Velocidad Tx.

En la figura 4.10.21, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 750 bytes, 1125 bytes y 1500 bytes los cuales han utilizado una velocidad de Tx constante de 0.5 Mbps, en la gráfica se puede observar claramente que al enviar una trama de 750 bytes se envía 84 pps, con una trama de 1125 se envía 56 pps y con una trama de 1500 se envía 41 pps.

Mientras en la figura 4.10.22, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 1470 bytes los cuales han utilizado una velocidad de Tx variada de: 0.5 Mbps, 1 Mbps y 2 Mbps, sin que se produzcan perdidas en el envío, como los datos que se muestran en la tabla 4.10.7.

PASO 3: Medición del Jitter

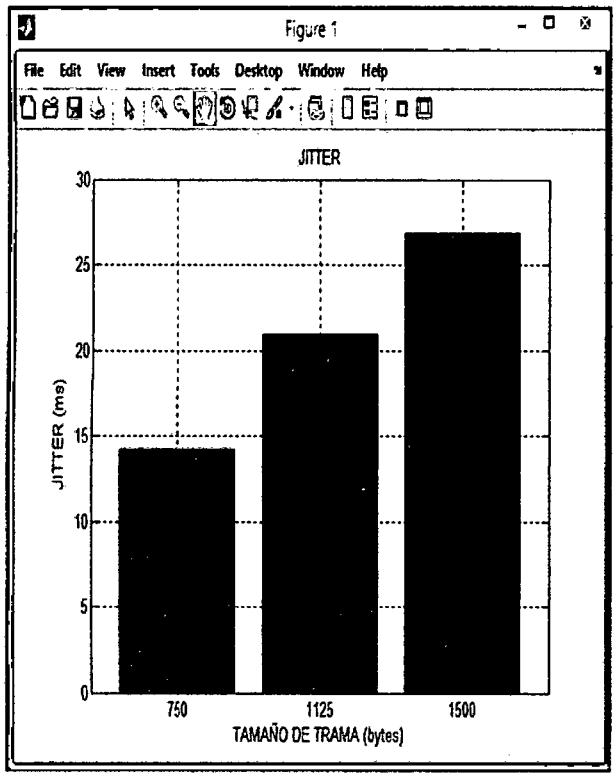
Para la medición se envió datos UDP de longitud variable a velocidades diferentes de Throughput obtenida anteriormente durante 20 segundos. Como se utilizó anteriormente Jperf el cliente será el encargado de enviar los datos y el servidor los recibirá, indicando los valores de Jitter obtenidos durante la transmisión de los datos.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**0.5**	**0.5**	**0.5**
Velocidad de Rx (Mbps)	**0.5**	**0.497**	**0.496**
Tramas Transmitidas	**834**	**557**	**418**
Tramas Recibidas	**834**	**557**	**418**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**14.226**	**20.982**	**26.823**

Tabla 4.10.8 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**0.5**	**1**	**2**
Velocidad de Rx (Mbps)	**0.5**	**0.924**	**1.21**
Tramas Transmitidas	**426**	**851**	**1701**
Tramas Recibidas	**426**	**851**	**1613**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**88 (5.2%)**
Jitter (ms)	**17.965**	**17.981**	**21.659**

Tabla 4.10.9 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.



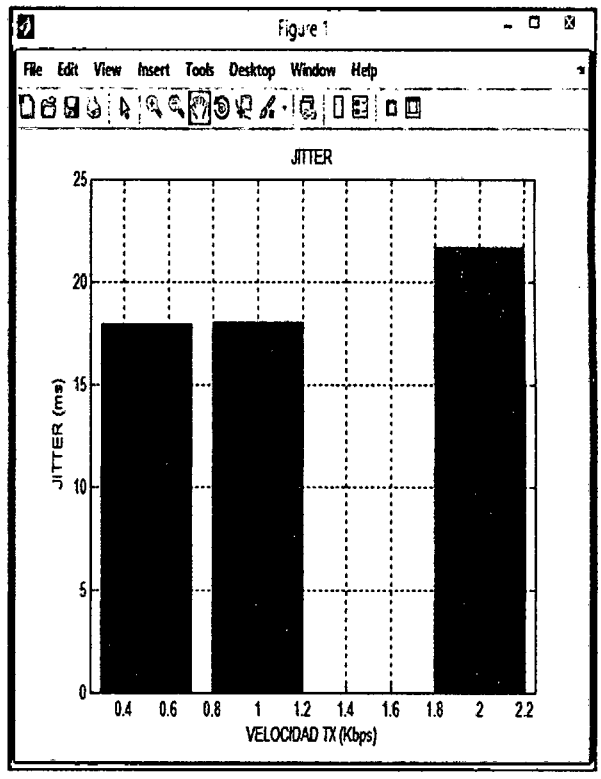


Fig. 4.10.23 Jitter vs. Tamaño de Trama **Fig. 4.10.24 Jitter vs. Velocidad Tx**

En la figura 4.10.23 se observa los valores del Jitter obtenidos al enviar diferentes tamaños de paquete UDP como 750, 1125 y 1500 bytes utilizando una velocidad de Tx constante de 0.5 Mbps, se puede observar claramente que con una trama de 750 bytes se tiene un Jitter de 14.22 ms a diferencia de la trama de 1500 bytes en la cual se tiene un Jitter de 26.82 ms.

En la figura 4.10.24, se observa los valores del Jitter obtenidos al enviar paquetes UDP de 1470 bytes utilizando una velocidad de Tx que varía entre 0.5 Mbps, 1 Mbps y 2 Mbps sin que se pierdan paquetes en la red, concluyendo también que a mayor ancho de banda mucho mayor será el jitter y pérdidas de datagramas.

Medición de Jitter a 500 kbps:

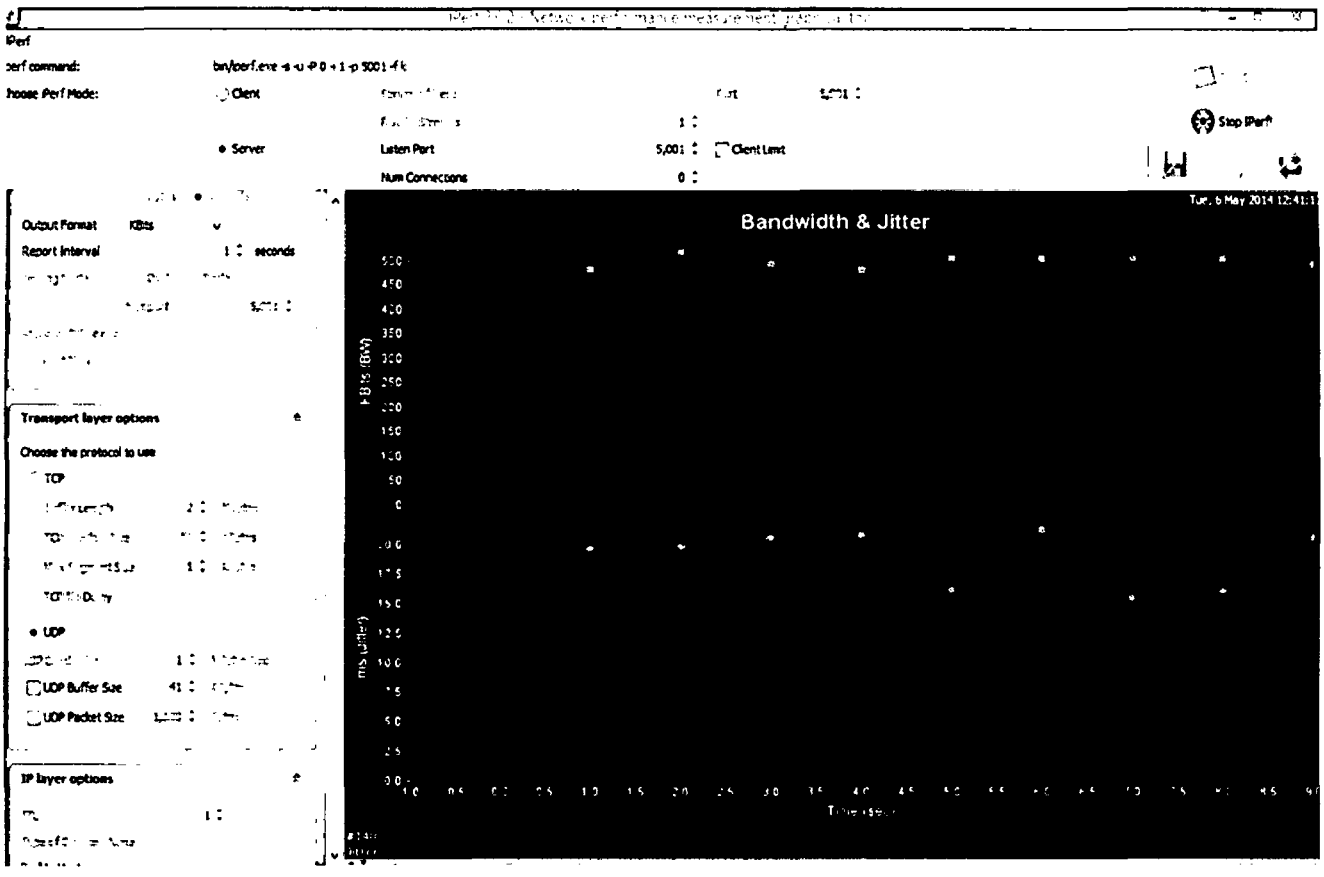


Fig. 4.10.25 Gráfica de Bandwidth y Jitter.

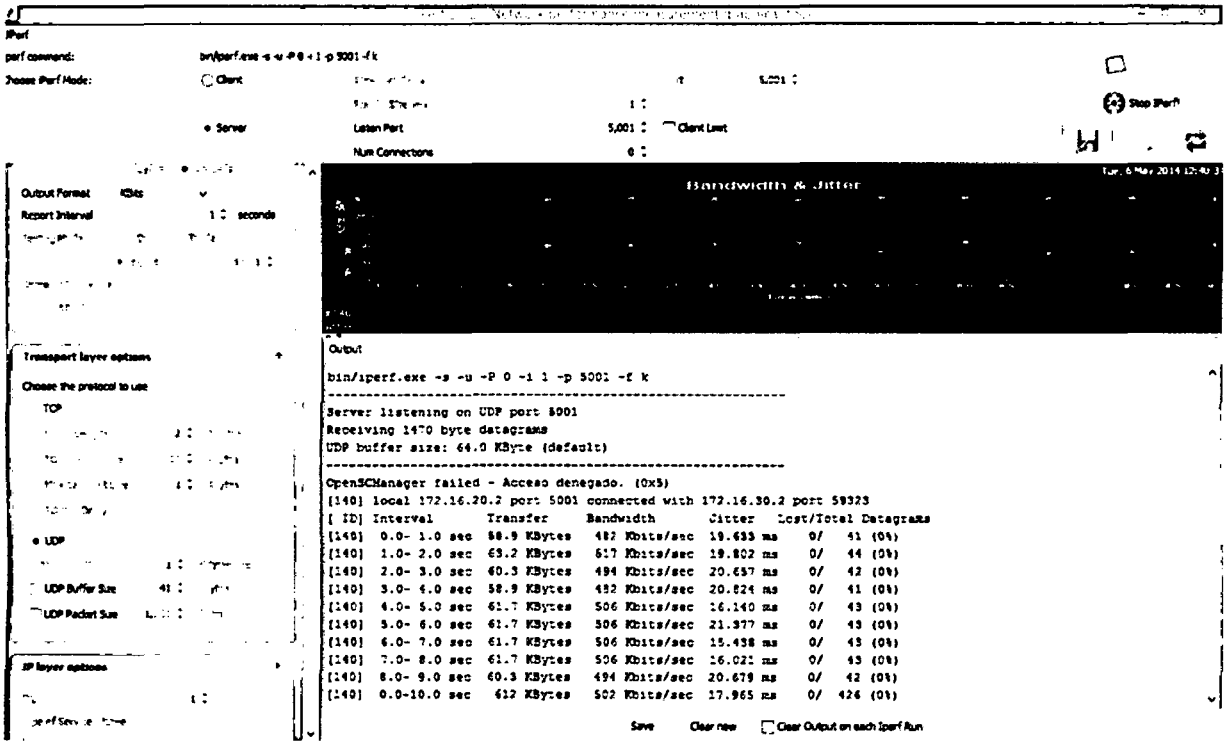


Fig. 4.10.26 Resultados al medir Throughput como servidor.

PASO 4: Captura de tráfico con Wireshark.

Capturar tráfico de paquetes en la interfaz s1/3 de R1.

- Captura de paquetes ICMP, vista de protocolos OSPF Y PPP:

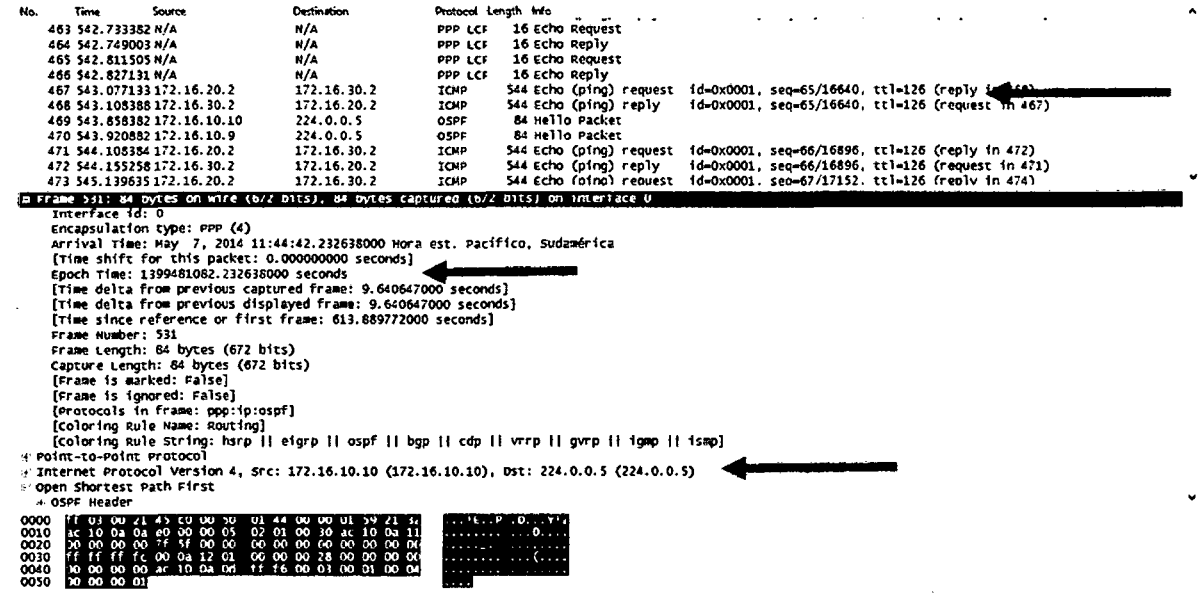


Fig. 4.10.27 Información de la encapsulación y autenticación PPP.

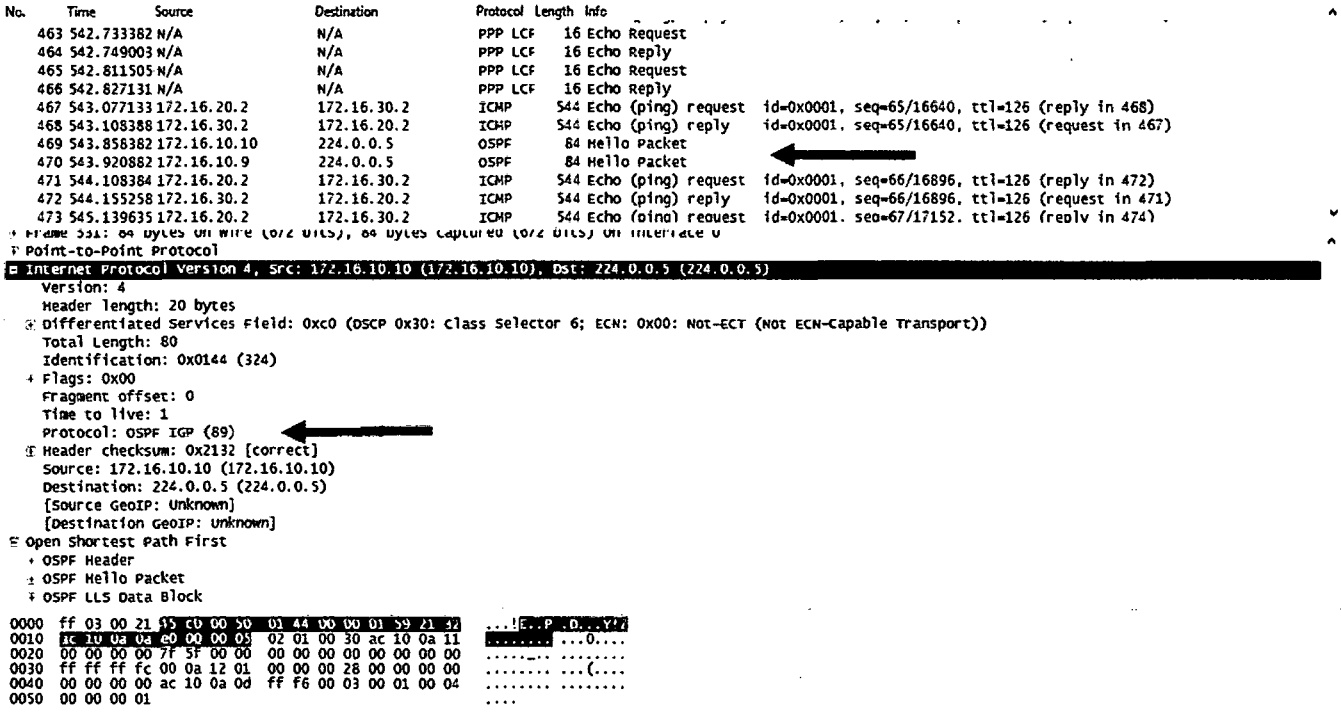


Fig. 4.10.28 Información detallada del origen y destino de paquetes.

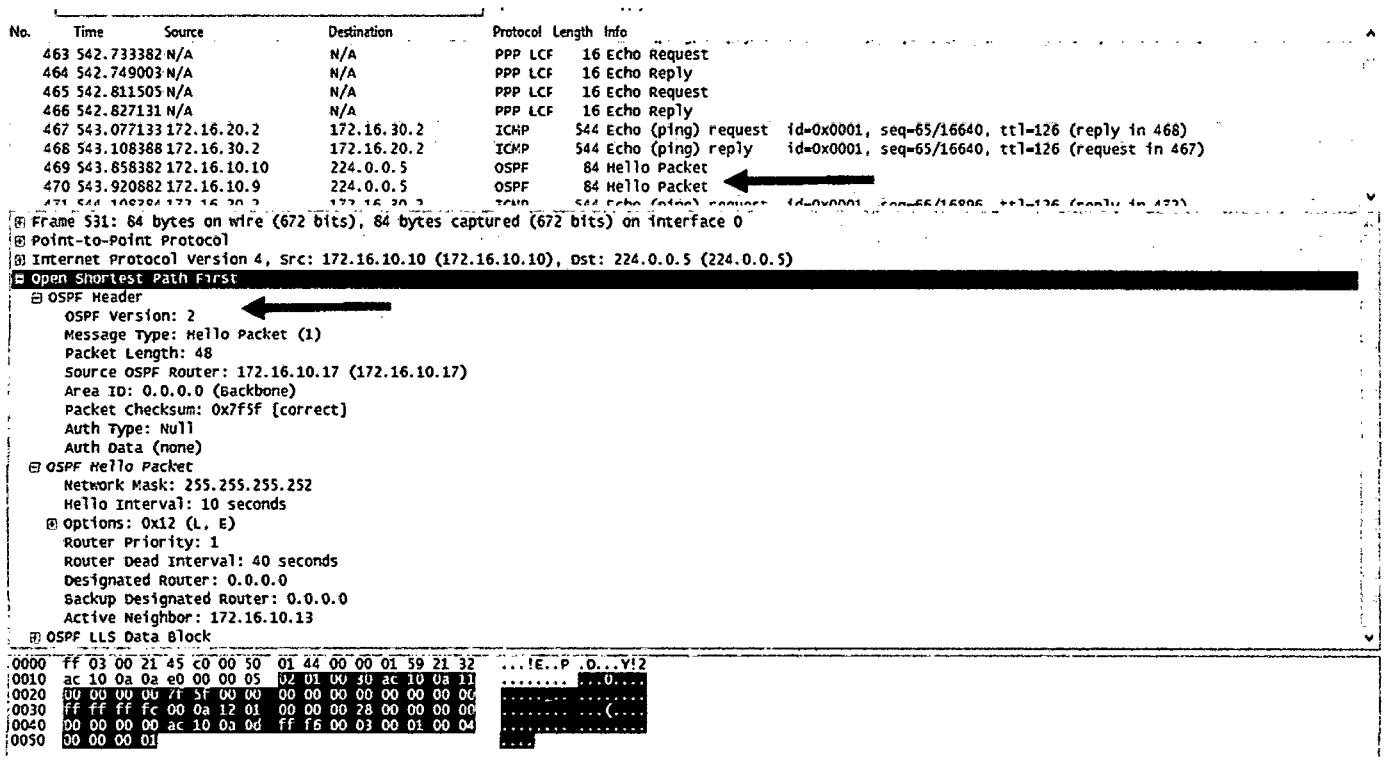


Fig. 4.10.29 Información detallada del protocolo OSPF.

PRÁCTICA DE LABORATORIO 4.11: CONFIGURACION BASICA DE FRAME RELAY

REVISIÓN TEÓRICA: Para la realización de esta práctica se deberá revisar conceptos de Frame Relay.

OBJETIVOS DE APRENDIZAJE

Al completar esta práctica de laboratorio, el usuario podrá:

- Conectar una red según el diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar interfaces.
- Configurar el enrutamiento EIGRP en todos los routers.
- Configurar la encapsulación Frame Relay en todas las interfaces seriales.
- Configurar una subinterfaz Frame Relay.
- Configurar un switch Frame Relay.
- Comprender los resultados de los comandos show frame-relay.
- Aprender los efectos del comando debug frame-relay lmi.
- Probar conectividad en la red y funcionamiento de Frame Relay.

ESCENARIO

En esta práctica de laboratorio, se aprenderá a configurar la encapsulación Frame Relay en enlaces seriales a través de la red que se muestra en el diagrama de topología. También se aprenderá a configurar un router con la encapsulacion Frame Relay y como configurar un switch Frame Relay. Existen estándares tanto de Cisco como abiertos que se aplican a Frame Relay. Se aprenderán ambos. Utilice la dirección 172.16.1.0/24 para obtener el direccionamiento IP usando VLSM, para los enlaces WAN entre routers y para los enlaces LAN utilice 172.16.2.0/24, 172.16.3.0/24 y 172.16.4.0/24 teniendo en cuenta los requisitos de las redes.

LAN R4: 200 host.

LAN R5: 140 host.

LAN R6: 180 host.

DIAGRAMA DE TOPOLOGIA:

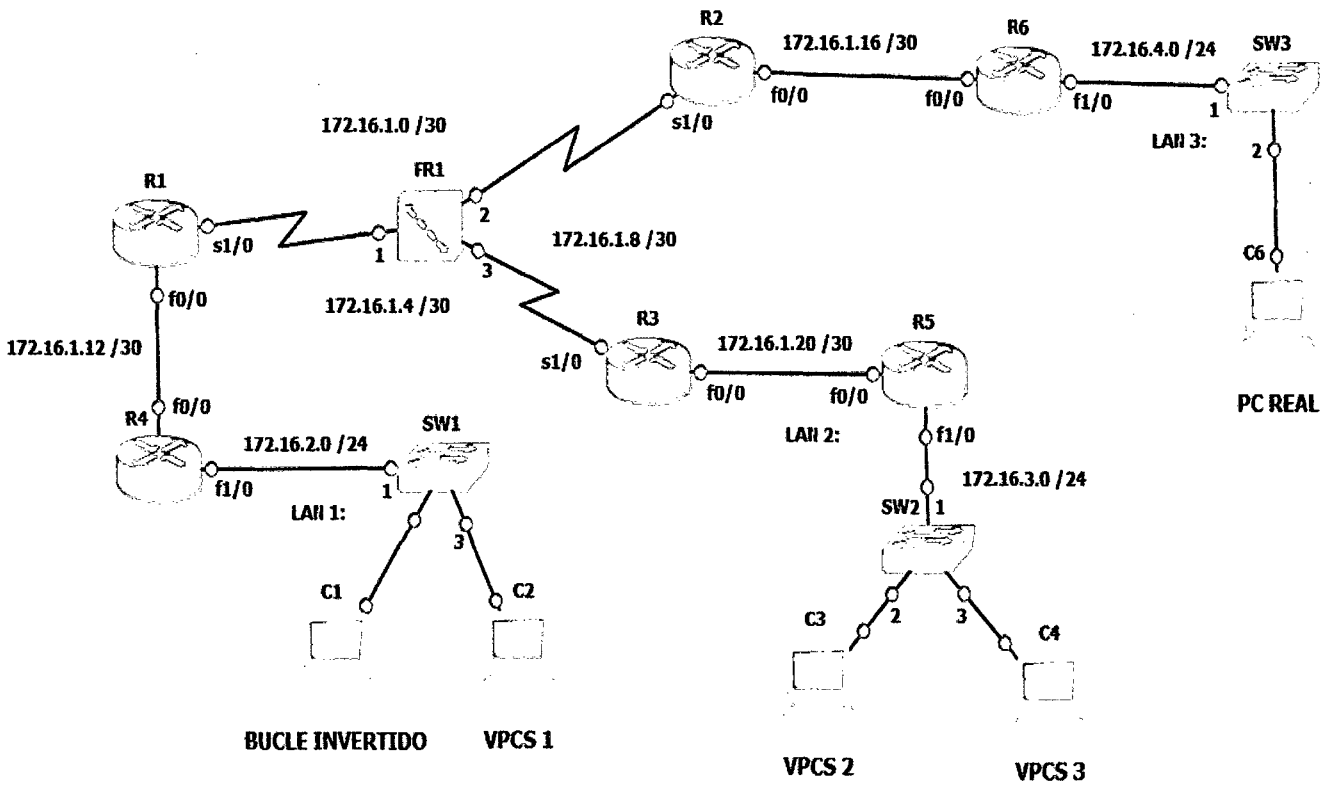


Fig. 4.11.1 Diagrama de topología en GNS3.

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN:

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s1/0.1	172.16.1.1	255.255.255.252	No aplicable
	s1/0.2	172.16.1.5	255.255.255.252	No aplicable
	f0/0	172.16.1.13	255.255.255. 252	No aplicable
R2	s1/0.1	172.16.1.2	255.255.255. 252	No aplicable
	s1/0.3	172.16.1.9	255.255.255. 252	No aplicable
	f0/0	172.16.1.17	255.255.255. 252	No aplicable
R3	s1/0.1	172.16.1.6	255.255.255. 252	No aplicable
	s1/0.2	172.16.1.10	255.255.255. 252	No aplicable
	f0/0	172.16.1.21	255.255.255. 252	No aplicable
R4	f0/0	172.16.1.14	255.255.255.252	No aplicable
	f1/0	172.16.2.1	255.255.255.0	No aplicable
R5	f0/0	172.16.1.22	255.255.255.252	No aplicable
	f1/0	172.16.3.1	255.255.255.0	No aplicable
R6	f0/0	172.16.1.18	255.255.255.252	No aplicable
	f1/0	172.16.4.1	255.255.255.0	No aplicable
C1	BUCLE INVERTIDO	172.16.2.2	255.255.255.0	172.16.2.1
C2	VPCS	172.16.2.3	255.255.255.0	172.16.2.1
C3	VPCS	172.16.3.2	255.255.255.0	172.16.3.1
C4	VPCS	172.16.3.3	255.255.255.0	172.16.3.1
PC REAL	NIC	172.16.4.2	255.255.255.0	172.16.4.1

Tabla 4.11.1 Direccionamiento IP para las Redes

TAREA 1: MONTAR LA RED EN GNS3

Montar y conectar la red igual a la del Diagrama de topología.

TAREA 2: REALIZAR LA CONFIGURACIÓN BÁSICA DEL ROUTER

Configure los routers R1, R2, R3, R4, R5 y R6 de acuerdo a las siguientes instrucciones desde el modo de configuración:

Paso 1: Configure el nombre de host del router.

Paso 2: Deshabilite la búsqueda DNS.

Paso 3: Configure una contraseña de Modo EXEC.

Paso 4: Configure un mensaje del día.

Paso 5: Configure una contraseña para las conexiones de la consola.

Paso 6: Configure una contraseña para las conexiones de vty.

Paso 7: Configure el registro de datos sincrónico.

Paso 8: Guardar la configuración en cada router.

TAREA 3: CONFIGURAR Y ACTIVAR LAS DIRECCIONES E INTERFACES FASTETHERNET

Configure todas las interfaces fastethernet de los routers R4, R5 y R6 con las direcciones IP de la tabla de direccionamiento que se encuentra al comienzo de esta práctica de laboratorio, en los routers R1, R2, R3 solo configure su interface fastethernet, sus interfaces seriales las configuraremos más adelante.

R4:

R4(config)#**interface fastethernet 0/0**

R4(config-if)#**ip address 172.16.1.14 255.255.255.252**

R4(config-if)#**description conexión a R1**

R4(config-if)#**no shutdown**

R4(config-if)#**exit**

R4(config)#**interface fastethernet 0/0**

R4(config-if)#**ip address 172.16.2.1 255.255.255.0**

R4(config-if)#**description conexión a LAN1**

R4(config-if)#**no shutdown**

R4(config-if)#**exit**

NOTA: Configuarar de igual manera las interfaces fastethernet faltantes de los routers.

TAREA 4: CONFIGURAR FRAME RELAY

Ahora se debe configurar una conexión Frame Relay punto a punto básica entre los routers 1, 2 y 3. Primero se debe configurar el switch Frame Relay y crear los DLCI.

Un PVC es un circuito virtual permanente, una conexión de la capa 2 creada entre extremos a través de un switch Frame Relay. Pueden existir varios PVC por interfaz física, lo que permite múltiples conexiones punto a punto o conexiones punto a multipunto. El siguiente paso es configurar los DLCI (Identificador de conexión de enlace de datos) en el switch Frame-Relay, para ello se debe hacer clic con el boton derecho sobre el switch y elegir configurar.

PASO 1: Configurar el switch Frame Relay.

Debemos agregar los siguientes DLCI

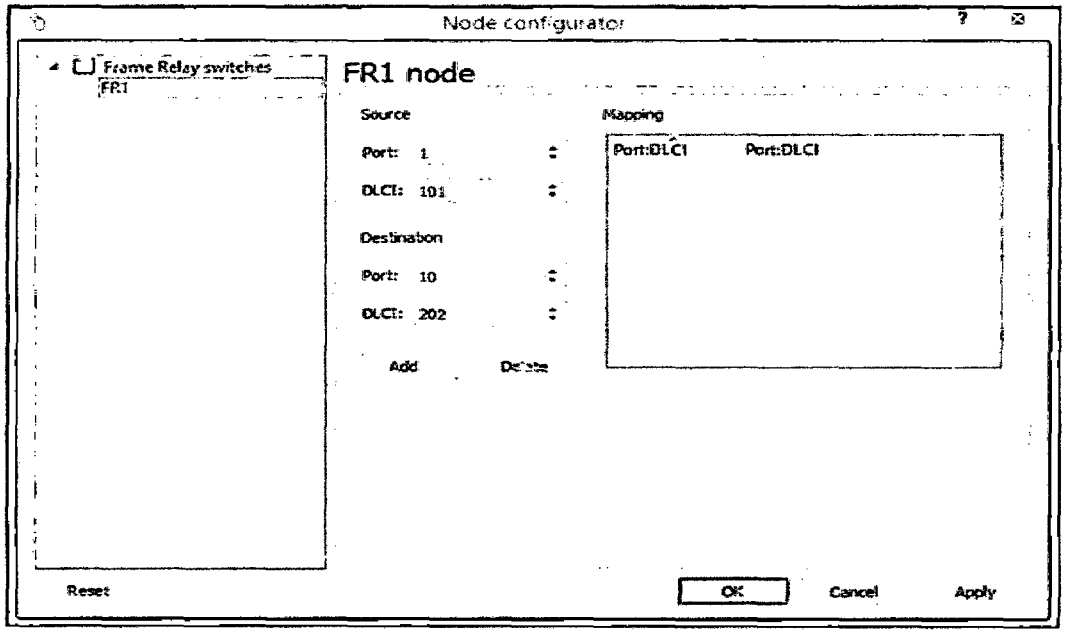


Fig. 4.11.2 Configuración del switch Frame Relay.

Origen: **Puerto: 1** **DLCI: 102** **Origen:** **Puerto: 1** **DLCI: 103**	**Destino:** **Puerto:2** **DLCI:201** **Destino:** **Puerto: 3** **DLCI: 301**
Origen: **Puerto: 2** **DLCI: 201** **Origen:** **Puerto: 2** **DLCI: 203**	**Destino:** **Puerto: 1** **DLCI: 102** **Destino:** **Puerto: 3** **DLCI: 302**
Origen: **Puerto: 3** **DLCI: 301** **Origen:** **Puerto: 3** **DLCI: 302**	**Destino:** **Puerto: 1** **DLCI: 103** **Destino:** **Puerto: 3** **DLCI: 203**

Tabla 4.11.2 Configuración de los DLCI en switch Frame Relay.

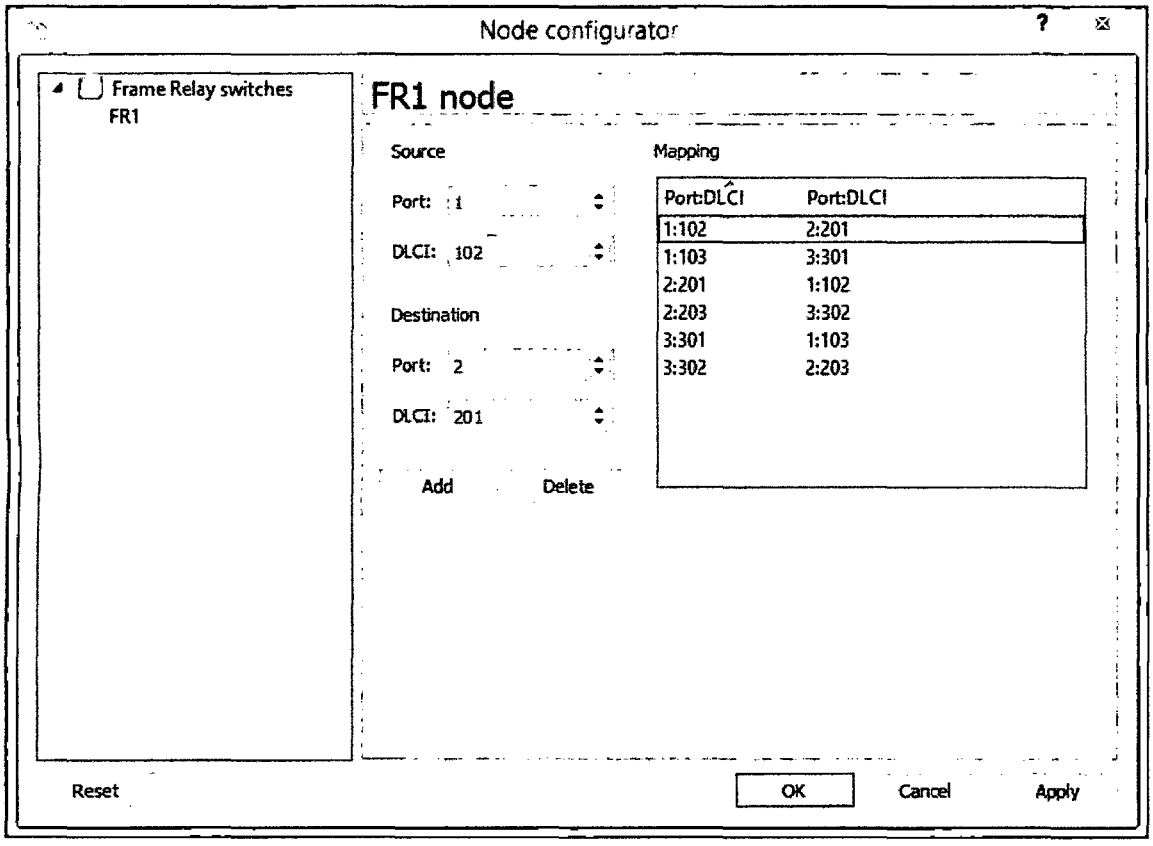


Fig. 4.11.3 Configuración de los DLCI en switch Frame Relay.

PASO 2: Configurar R1 para Frame Relay.

Lo único que faltaria sería conectar los router con el switch frame relay con sus correspondientes DLCI.

R1:

R1#configure terminal

R1(config)#interface serial 1/0

R1(config-if)#encapsulation frame-relay

R1(config-if)#no shutdown

R1(config-if)#interface serial 1/0.1 point-to-point

R1(config-subif)#ip address 172.16.1.1 255.255.255.252

R1(config-subif)#frame-relay interface-dlci 102

R1(config-fr-dlci)#interface serial 1/0.2 point-to-point

R1(config-subif)#ip address 192.168.100.5 255.255.255.252

R1(config-subif)#frame-relay interface-dlci 103

R2:

R2#configure terminal

R2(config)#interface serial 1/0

R2(config-if)#encapsulation frame-relay

R2(config-if)#no shutdown

R2(config-if)#interface serial 1/0.1 point-to-point

R2(config-subif)#ip address 172.16.1.2 255.255.255.252

R2(config-subif)#frame-relay interface-dlci 201

R2(config-if)#interface serial 1/0.3 point-to-point

R2(config-subif)#ip address 172.168.1.9 255.255.255.252

R2(config-subif)#frame-relay interface-dlci 203

R3:

R3#configure terminal

R3(config)#interface serial 1/0

R3(config-if)#encapsulation frame-relay

R3(config-if)#no shutdown

R3(config-if)#interface serial 1/0.1 point-to-point

R3(config-subif)#ip address 172.16.1.6 255.255.255.252

R3(config-subif)#frame-relay interface-dlci 301

R3(config-if)#interface serial 1/0.2 point-to-point

R3(config-subif)#ip address 172.16.1.10 255.255.255.252

R3(config-subif)#frame-relay interface-dlci 302

TAREA 5: CONFIGURAR EL PROTOCOLO EIGRP EN LOS ROUTERS

R3:

R3(config)#**router eigrp 100**

R3(config-router)#**network 172.16.1.20 0.0.0.3**

R3(config-router)#**network 172.16.1.4 0.0.0.3**

R3(config-router)# **network 172.16.1.8 0.0.0.3**

R3(config-router)#**no auto-summary**

R3(config-router)#**exit**

R6:

R6(config)#**router eigrp 100**

R6(config-router)#**network 172.16.1.16 0.0.0.3**

R6(config-router)#**network 172.16.4.0 0.0.0.255**

R6(config-router)# **passive-interface fastethernet 1/0**

R6(config-router)#**no auto-summary**

R6(config-router)#**exit**

NOTA: Configurar de igual forma los router faltantes.

TAREA 6: CONFIGURAR LOS EQUIPOS DE HOST.

Configurar las direcciones IP y gateways por defecto como se indican en la tabla de direccionamiento de las interfaces Ethernet de C1, C2, C3 y C4 (VPCS) y PC REAL.

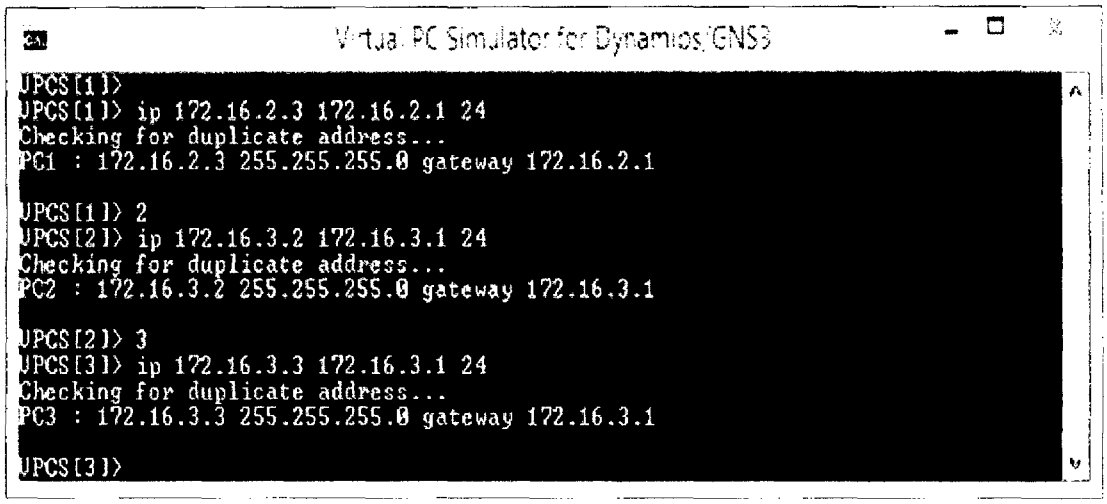


Fig. 4.11.4 Configuración de las direcciones IP en el VPCS.

TAREA 7: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

PASO 1: Verificar el direccionamiento IP y las interfaces.

R1#**show ip interface brief**

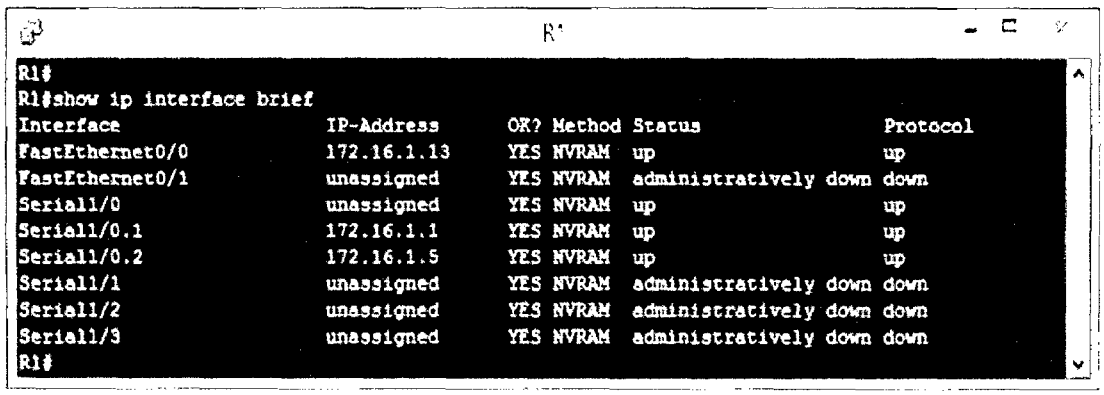


Fig. 4.11.5 Tabla ip de interface brief de R1.

NOTA: Verificar que las interfaces de los demás routers tengan la adecuada dirección IP y estén activas.

PASO 2: Verificar la configuración de los router. Use los comandos **show ip route** para verificar el contenido de la tabla de enrutamiento.

R1#**show ip route**

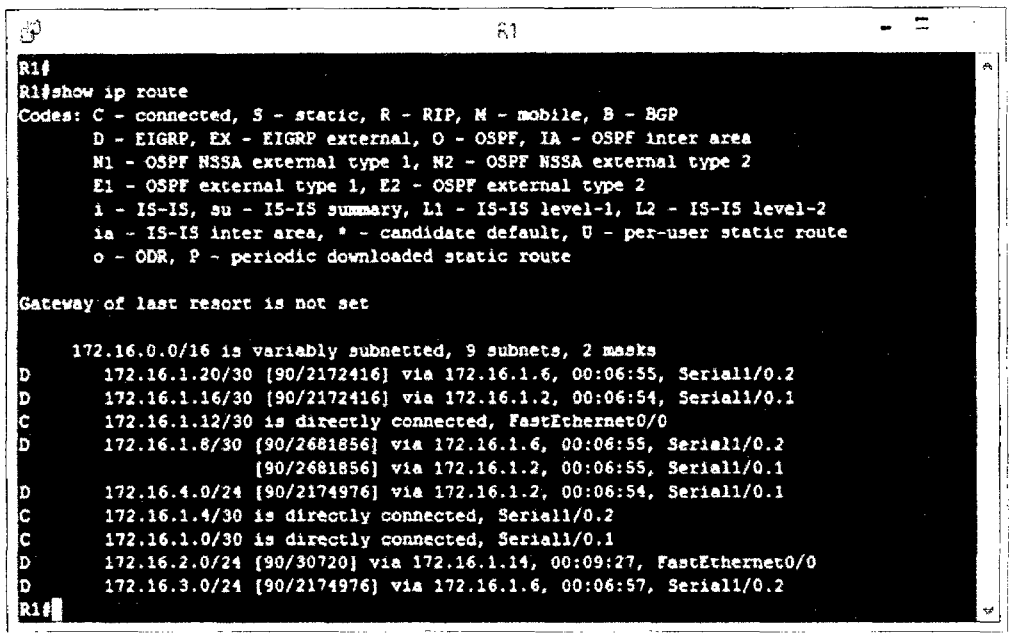


Fig. 4.10.6 Tabla de enrutamiento de R1.

NOTA: Verificar de igual manera la tabla de enrutamiento de los demás routers.

PASO 3: Una vez que hemos configurado la encapsulación Frame Relay en las subinterfaces de los routers, verificaremos su configuración con el comando **show interface serial**, como se muestra a continuación.

R1#**show interface serial 1/0.1**

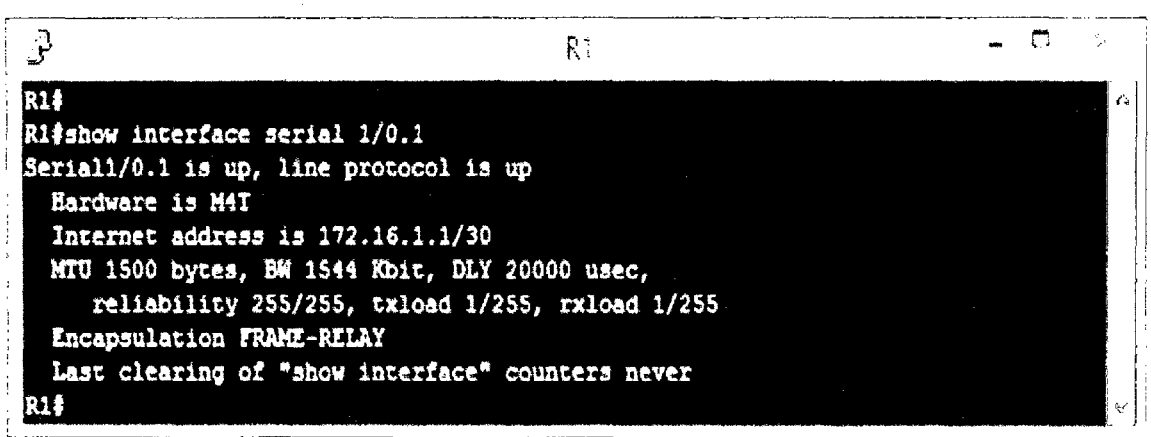


Fig. 4.11.7 Verificación de la encapsulación Frame Relay en la subinterface 1/0.1.

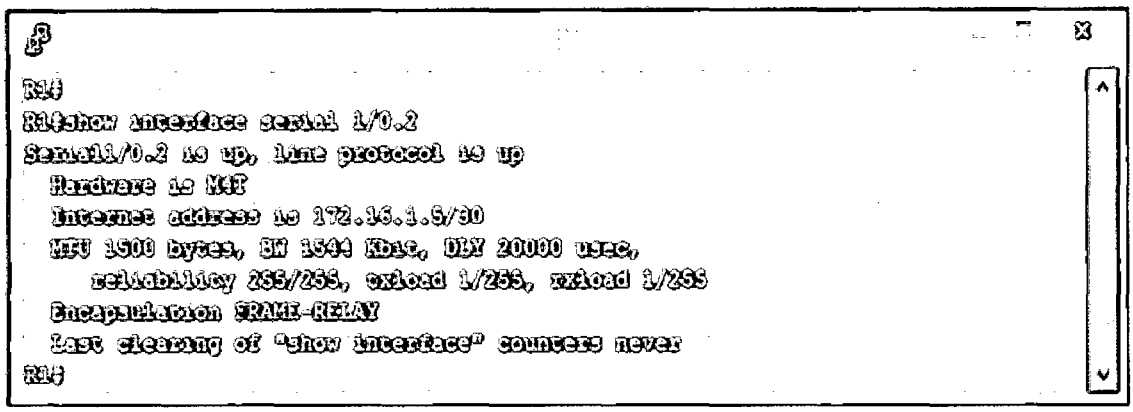


Fig. 4.11.8 Verificación de la encapsulación Frame Relay en la subinterface 1/0.2.

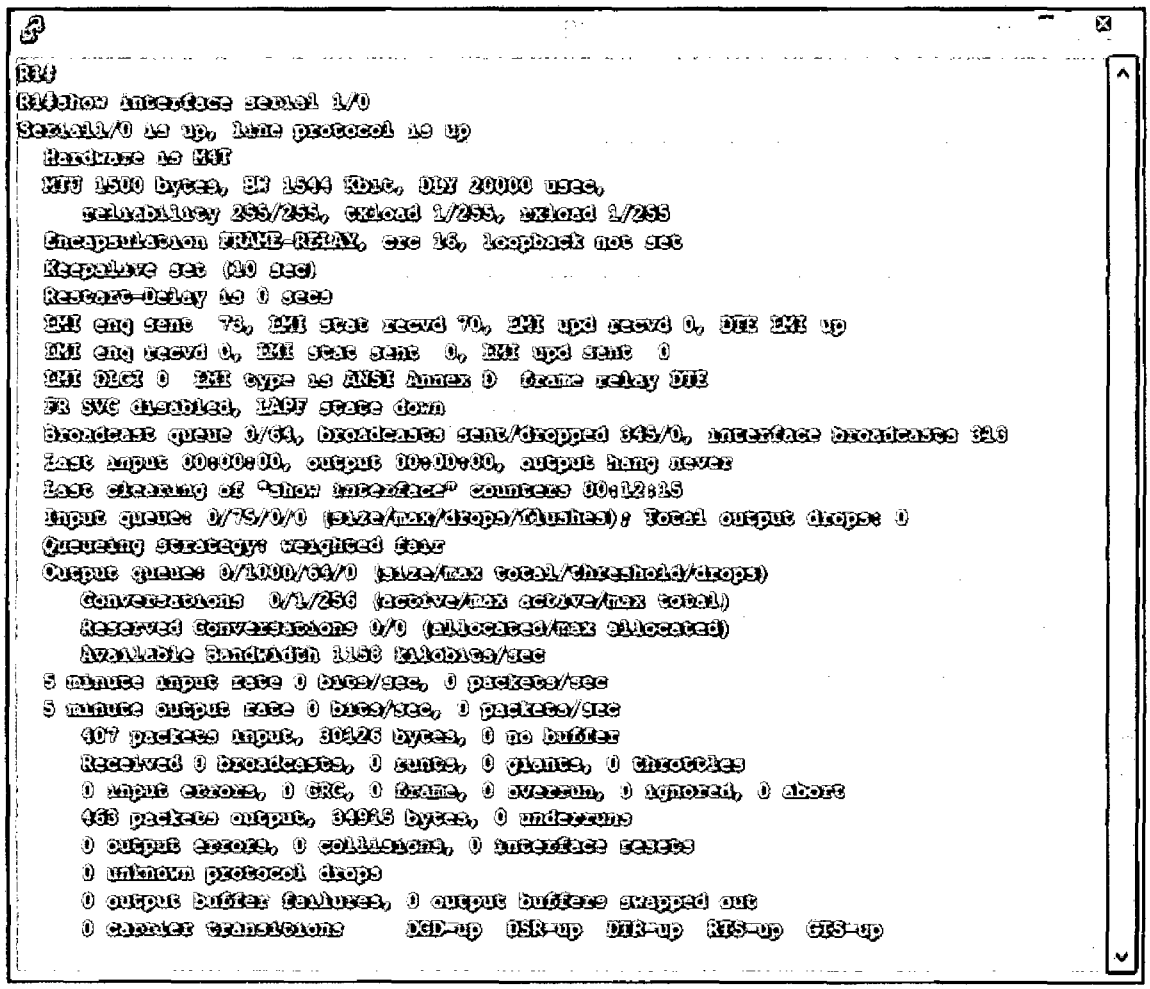


Fig. 4.11.9 Verificación de la encapsulación Frame Relay en la interface 1/0.

NOTA: Verificar la encapsulación Frame Relay en los routers R2 y R3.

PASO 4: verificaremos la configuración de Frame Relay con los comandos que se muestra a continuación.

-show frame-relay map

- show frame-relay pvc

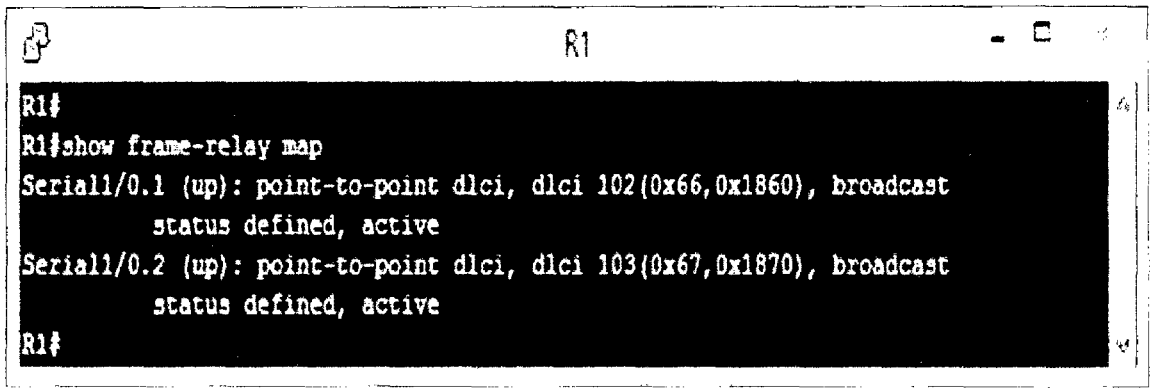


Fig. 4.11.10 Verificación de Frame Relay en el router R1.

NOTA: Verificar la configuración de Frame Relay en los routers R2 y R3.

PASO 5: Verificar que hay conectividad completa en la red.

Use el comando **ping** para verificar la conectividad.

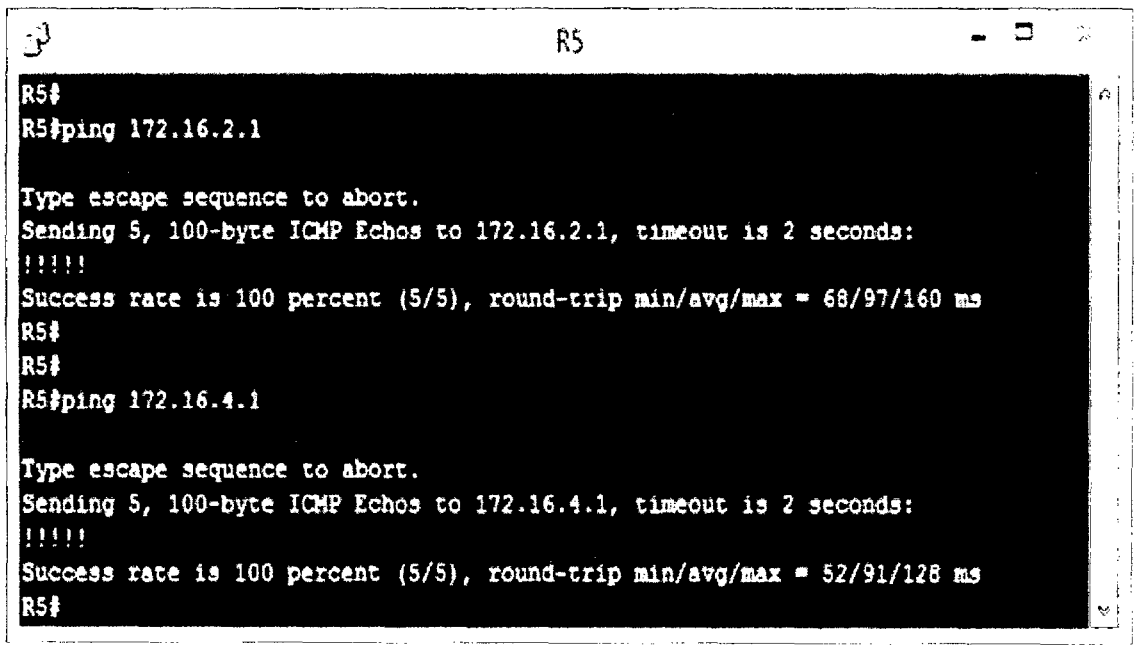


Fig. 4.11.11 Prueba de conectividad entre routers.

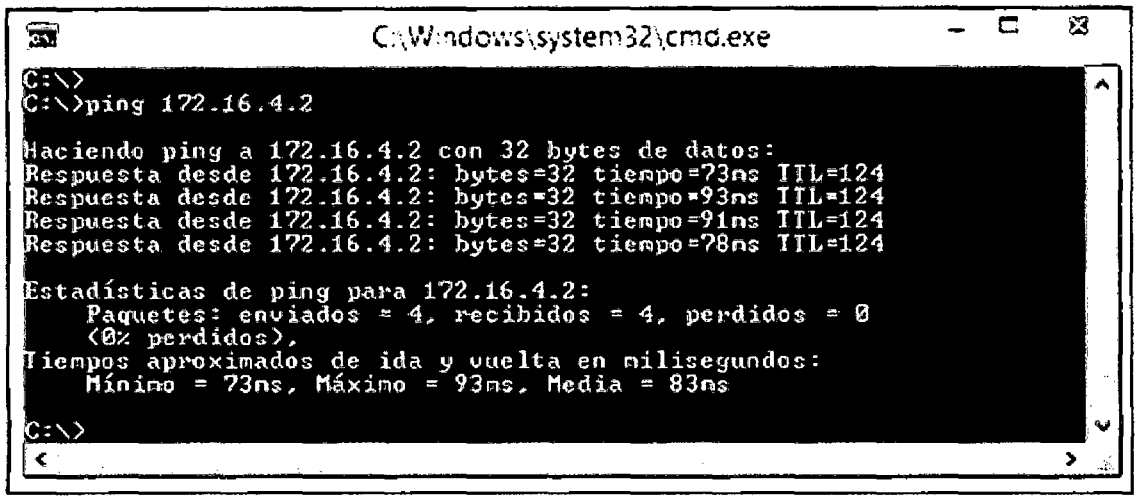


Fig. 4.11.12 Prueba de conectividad entre host desde C1 a PC real.

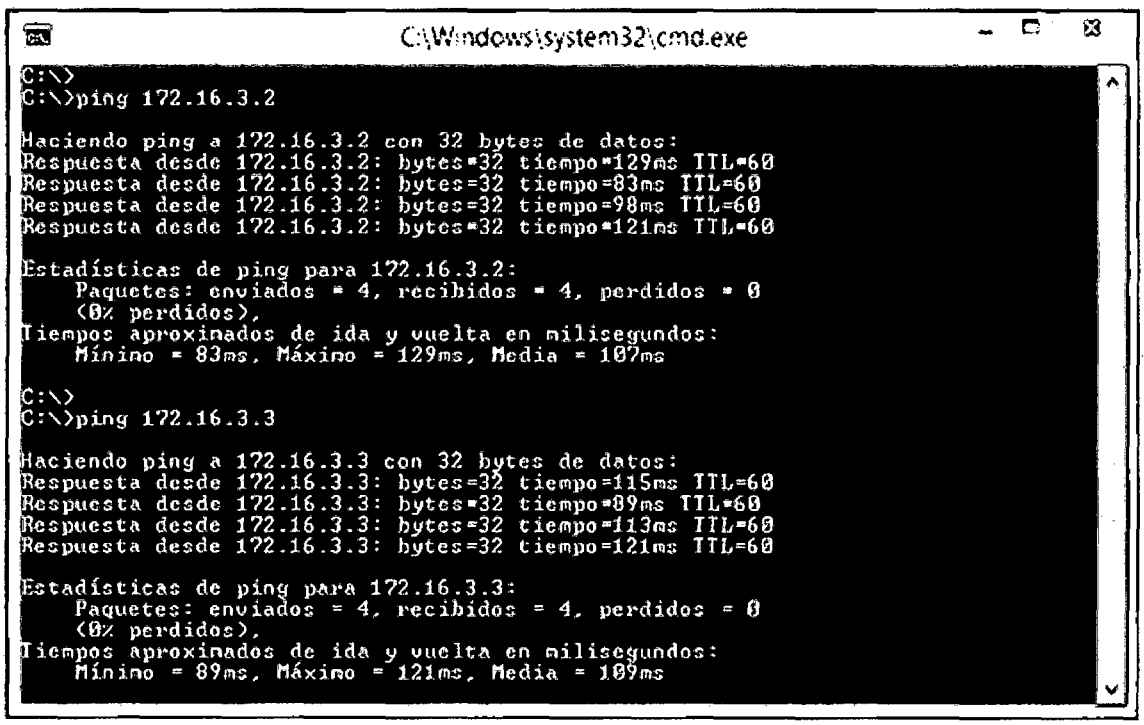


Fig. 4.11.13 Prueba de conectividad entre host desde C2 a PC real.

TAREA 8: ANALISIS DEL TRAFICO DE PAQUETES

PASO 1: Medición de la Latencia

Para la medición de la latencia se realizó 10 muestras sucesivas de 100 ping desde el C1 (Bucle invertido) hacia la PC REAL considerando un tamaño de trama de 64, 512 y 1518 bytes como se especifica en el RFC 2544.

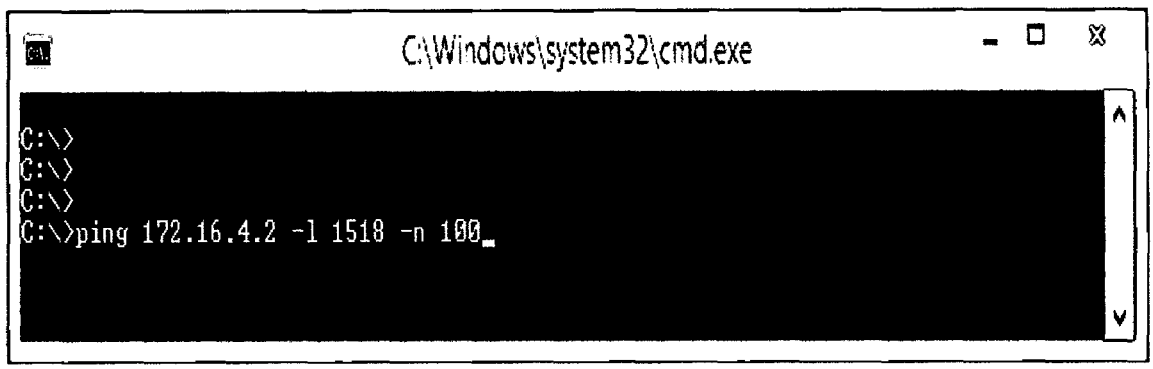


Fig. 4.11.14 Forma de medición de la latencia.

En la Figura 4.11.14 se puede observar el envío de 100 ping con una trama de 1518 hacia la dirección 172.16.4.2

En las Tablas posteriores se detallan los valores de la Latencia que se ha obtenido una vez realizadas todas las muestras.

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	**60**	**60**	**53**	**64**	**56**	**65**	**66**	**62**	**60**	**58**	**60.4**
Tiempo Máximo (ms)	**104**	**114**	**182**	**210**	**89**	**250**	**252**	**251**	**80**	**121**	**165.3**
Tiempo Promedio (ms)	**75**	**74**	**80**	**122**	**70**	**134**	**107**	**123**	**71**	**75**	**93.1**

Tabla 4.11.3 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	512										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	61	57	62	62	62	62	59	60	63	64	61.2
Tiempo Máximo (ms)	232	103	104	330	267	113	342	90	210	92	188.3
Tiempo Promedio (ms)	119	71	75	122	108	76	135	74	120	78	97.8

Tabla 4.11.4 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1518										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	67	65	65	64	67	66	68	69	67	73	67.1
Tiempo Máximo (ms)	108	103	232	262	285	252	291	257	236	264	229
Tiempo Promedio (ms)	81	78	118	114	121	133	120	143	135	135	117.8

Tabla 4.11.5 Comparación de datos obtenidos de las diferentes tramas.

LATENCIA			
Tamaño de Trama (bytes)	64	512	1518
Tiempo Mínimo (ms)	60.4	61.2	67.1
Tiempo Máximo (ms)	165.3	188.3	229
Tiempo Promedio (ms)	93.1	97.8	117.8

Tabla 4.11.6 Comparación de datos obtenidos de las diferentes tramas.

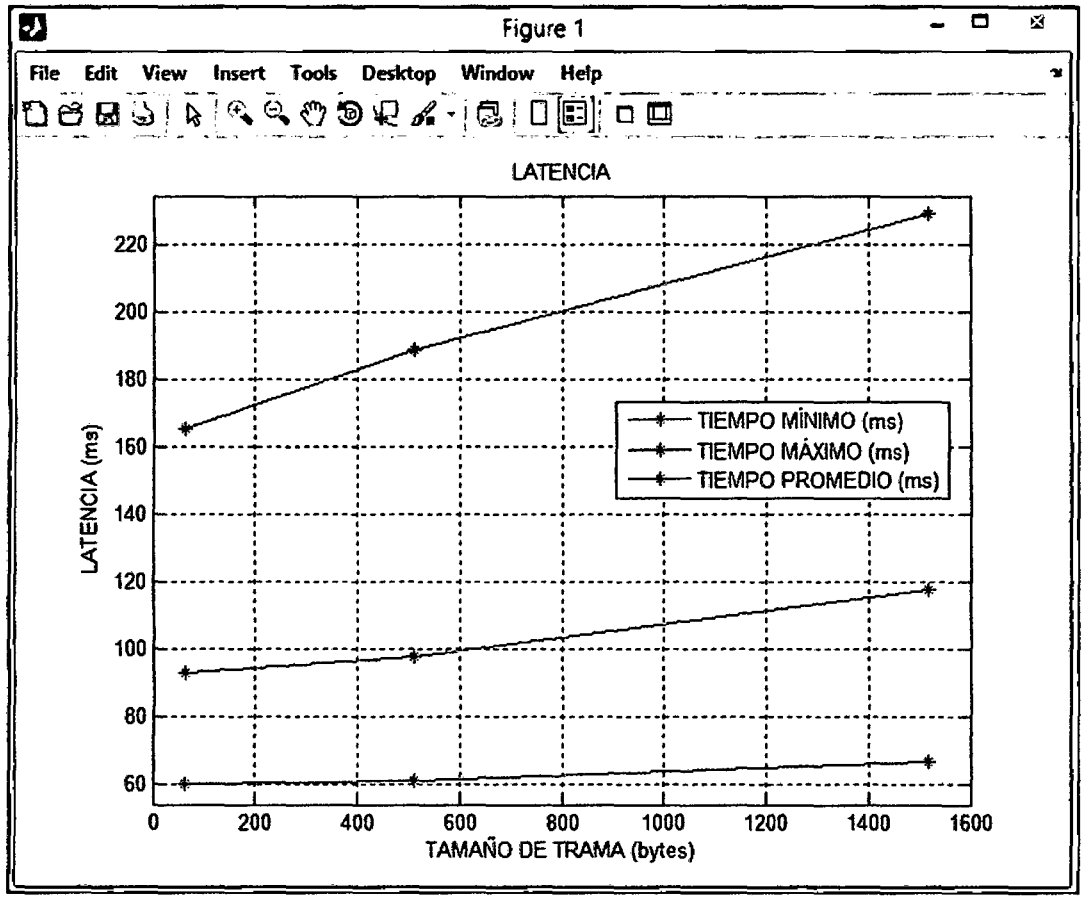


Fig. 4.11.15 Datos representados gráficamente de la variación de la latencia.

De acuerdo con los datos obtenidos, se puede observar claramente que los valores mínimo (color azul), máximo (color rojo) y promedio (color verde) de la latencia de la red se incrementan conforme se envía una trama de longitud mayor, en este caso con la trama de 1518 bytes se obtiene una latencia promedio de 117.8 ms a diferencia de una trama de 64 bytes con 93.1 ms.

PASO 2: Medición del Throughput

Para la medición del Throughput y Jitter se envió una cantidad de tramas a velocidades diferentes durante 20 segundos, hasta encontrar la máxima cantidad de tramas recibidas sin que se produzcan perdidas de las mismas en el router y PC REAL. Como se utilizó Jperf el cliente será el encargado de enviar los paquetes y el servidor los recibirá, indicando la cantidad de paquetes que llegaron correctamente considerando un tamaño del paquete UDP de 750, 1125, 1500 y 1470 (default) bytes, tal como se especifica en el RFC 768.

Configuración del Jperf como servidor para medir Throughput:

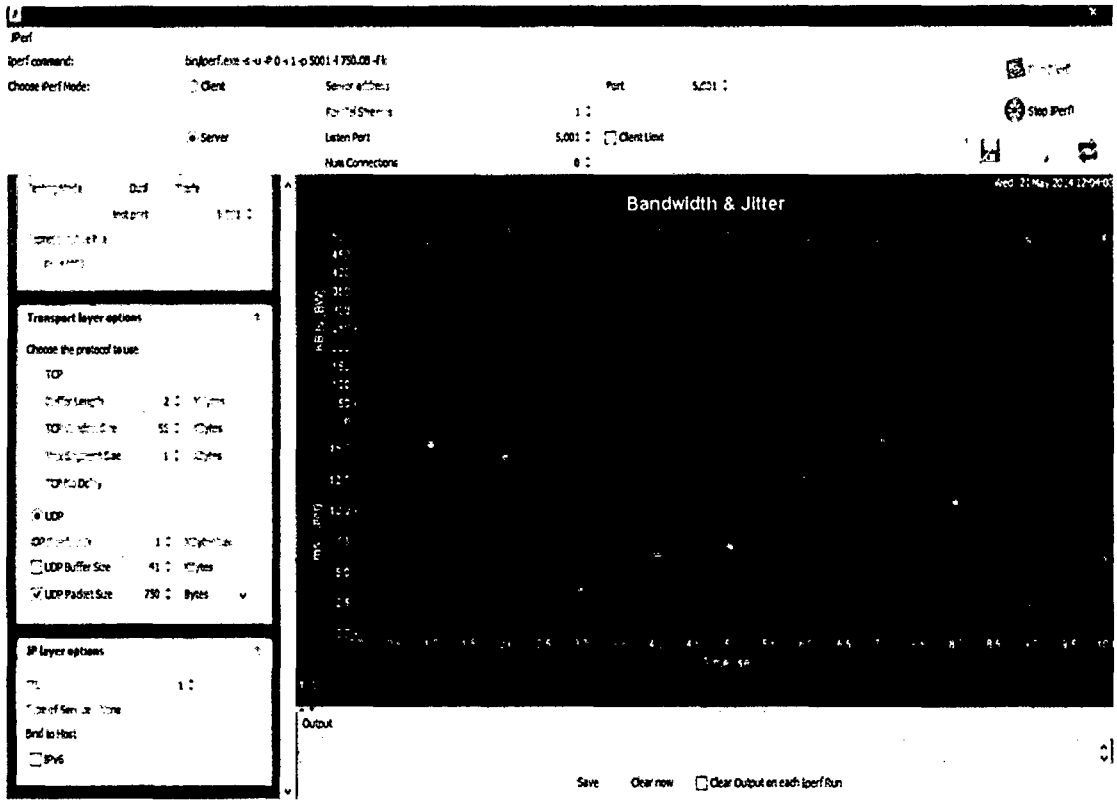


Fig. 4.11.16 Gráfica de Bandwidth y Jitter.

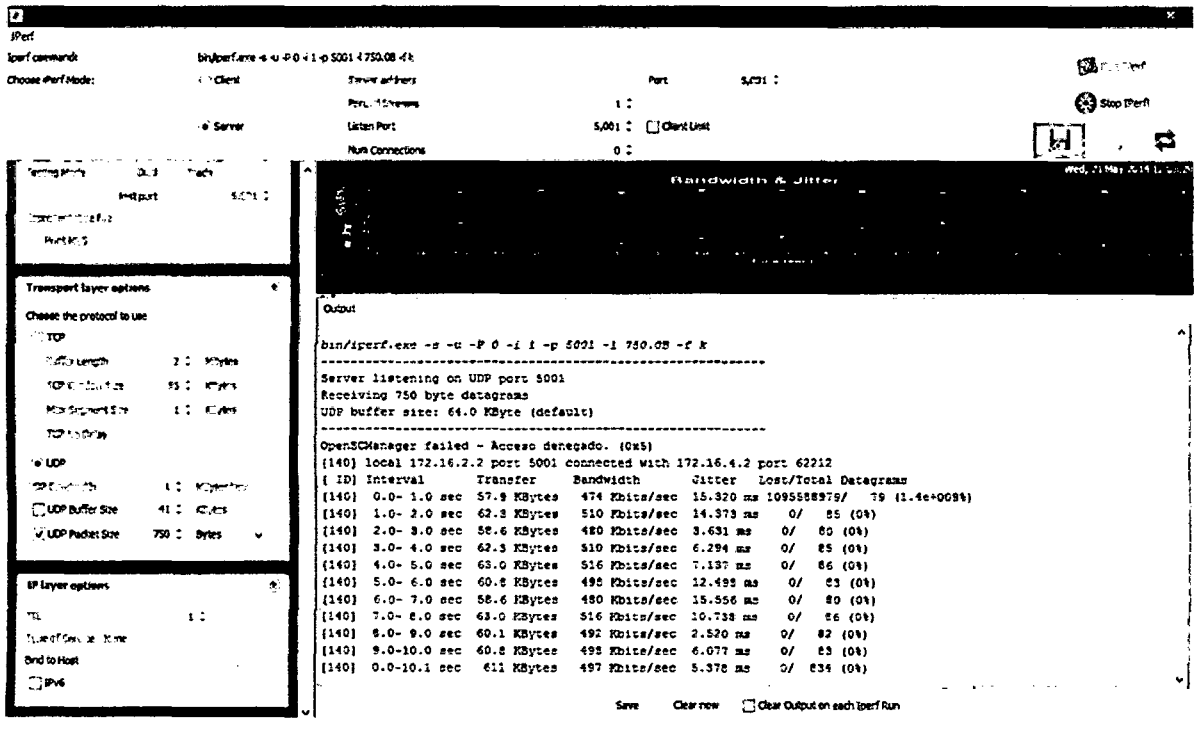


Fig. 4.11.17 Resultados al medir Throughput como servidor.

Configuración del Jperf como cliente para medir Throughput:

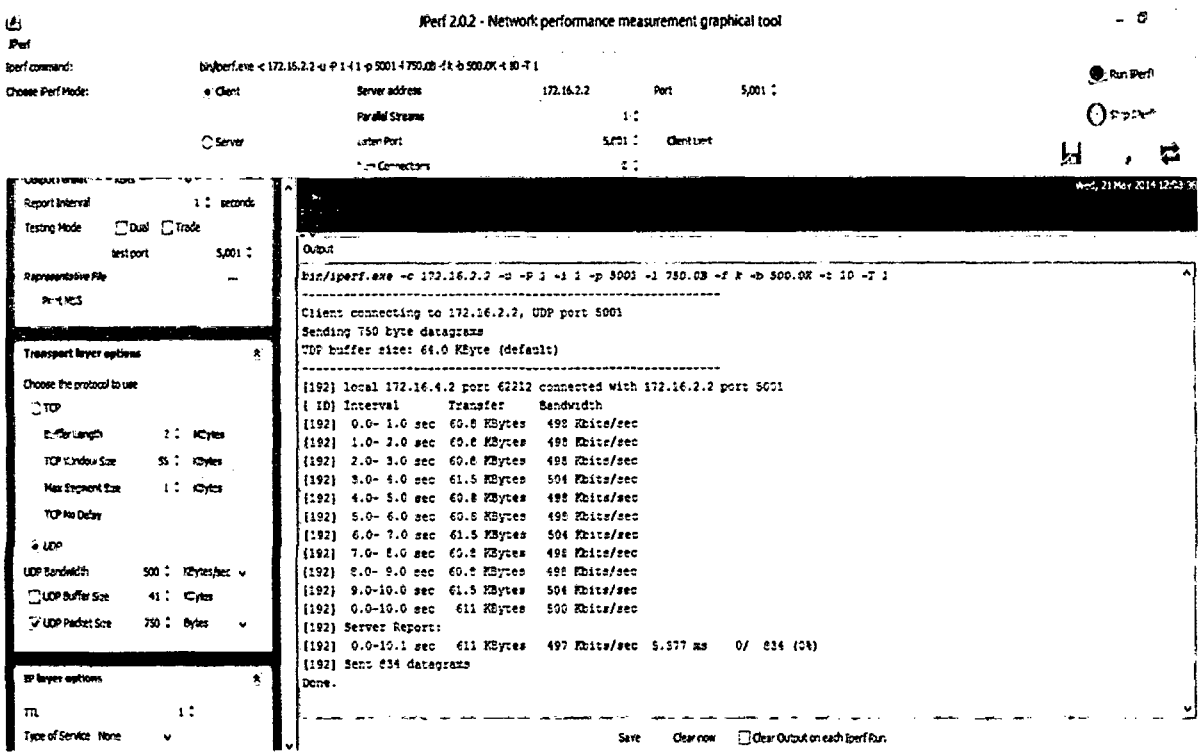


Fig. 4.11.18 Resultados del Jperf como Cliente al medir Throughput.

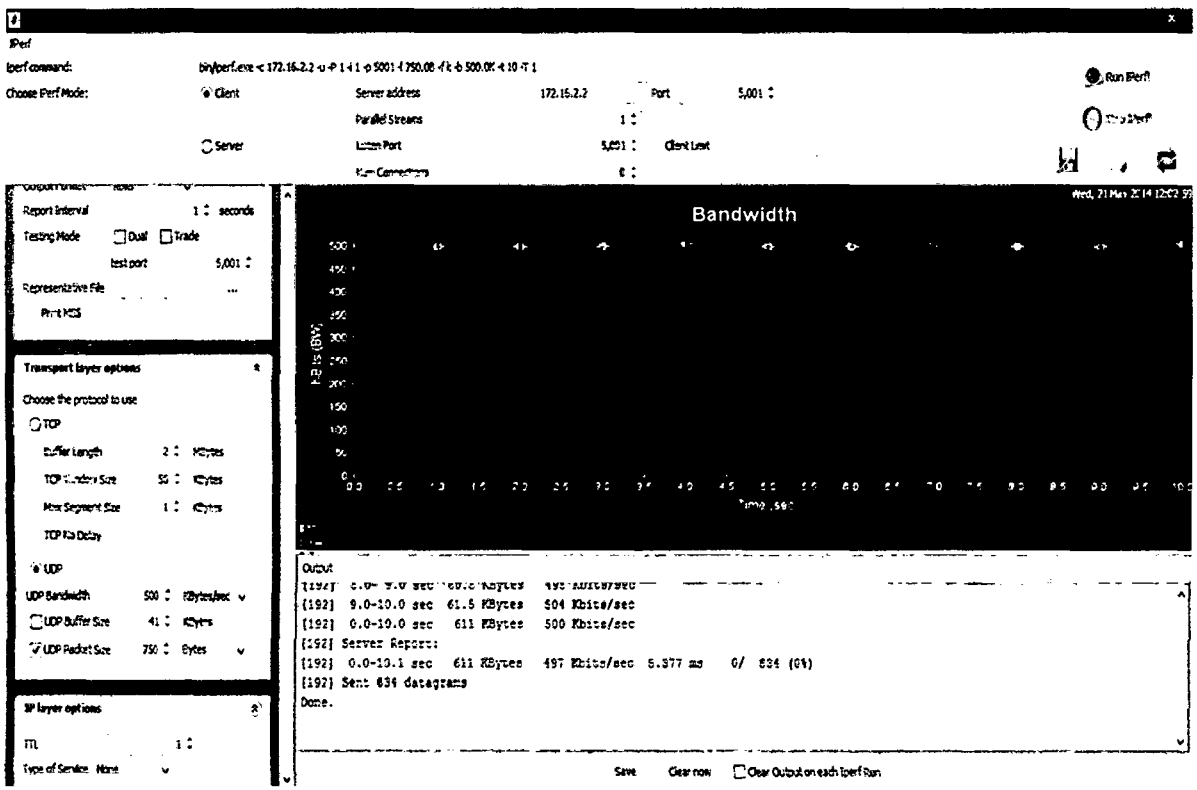


Fig. 4.11.19 Gráfica de Bandwidth

En las siguientes Tablas se detalla los valores del Throughput obtenidos una vez realizada todas las muestras.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**0.5**	**0.5**	**0.5**
Velocidad de Rx (Mbps)	**0.49**	**0.5**	**0.5**
Tramas Transmitidas	**834**	**556**	**418**
Tramas Recibidas	**834**	**556**	**418**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**83**	**55**	**41**

Tabla 4.11.7 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**0.5**	**1**	**2**
Velocidad de Rx (Mbps)	**0.49**	**1**	**2**
Tramas Transmitidas	**426**	**851**	**1700**
Tramas Recibidas	**426**	**851**	**1700**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**43**	**85**	**170**

Tabla 4.11.8 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

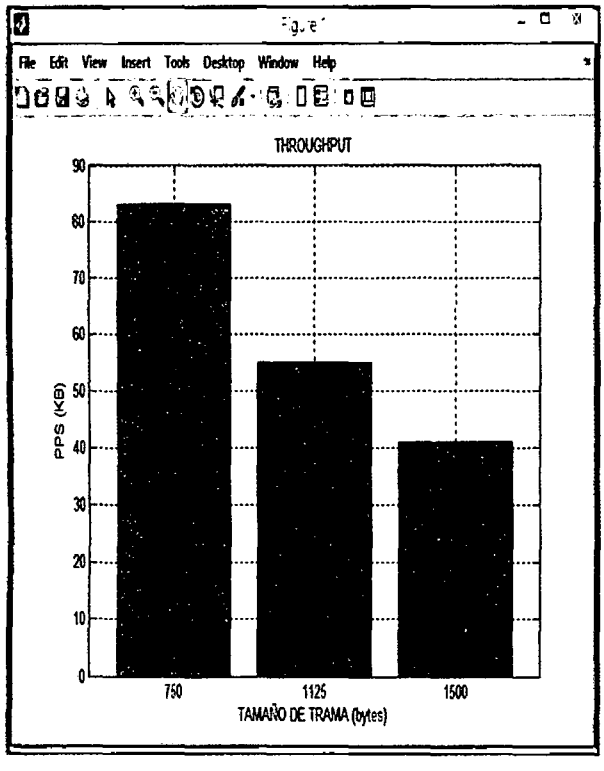


Fig. 4.11.20 PPS vs. Tamaño de Trama.

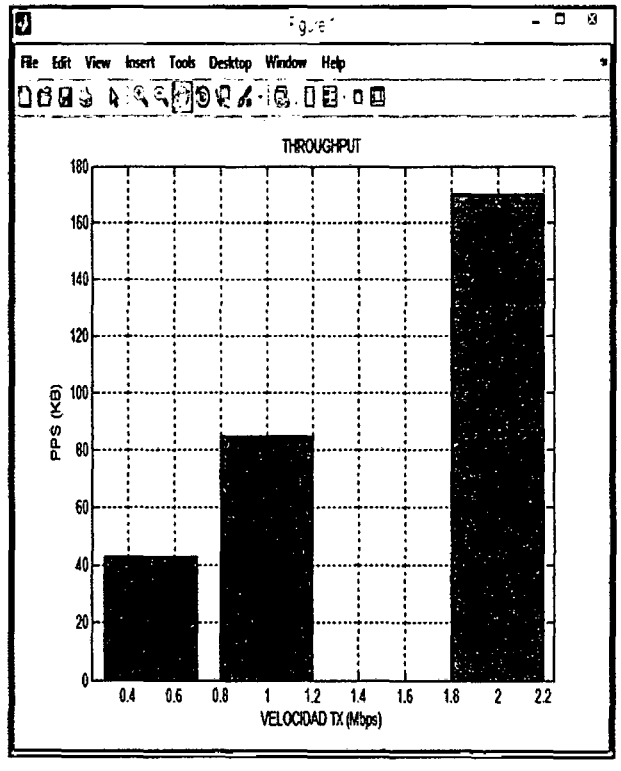


Fig. 4.11.21 PPS vs. Velocidad Tx.

En la figura 4.11.20, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 750 bytes, 1125 bytes y 1500 bytes los cuales han utilizado una velocidad de Tx constante de 0.5 Mbps, en la gráfica se puede observar claramente que al enviar una trama de 750 bytes se envía 83 pps, con una trama de 1125 se envía 55 pps y con una trama de 1500 se envía 41 pps.

Mientras en la figura 4.11.21, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 1470 bytes los cuales han utilizado una velocidad de Tx variada de: 0.5 Mbps, 1 Mbps y 2 Mbps, sin que se produzcan perdidas en el envío, como los datos que se muestran en la tabla 4.11.8.

PASO 3: Medición del Jitter

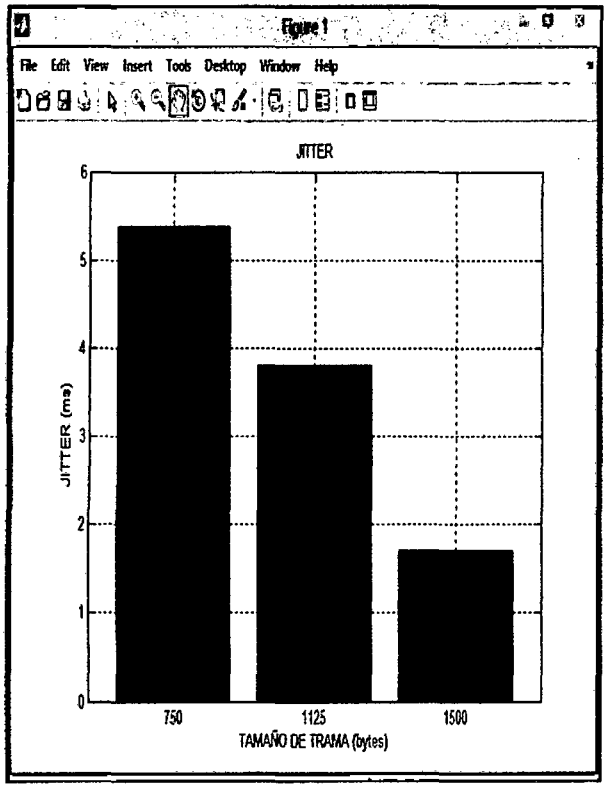
Para la medición se envió datos UDP de longitud variable a velocidades diferentes de Throughput obtenida anteriormente durante 20 segundos. Como se utilizó anteriormente Jperf el cliente será el encargado de enviar los datos y el servidor los recibirá, indicando los valores de Jitter obtenidos durante la transmisión de los datos.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**0.5**	**0.5**	**0.5**
Velocidad de Rx (Mbps)	**0.49**	**0.5**	**0.5**
Tramas Transmitidas	**834**	**556**	**418**
Tramas Recibidas	**834**	**556**	**418**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**5.378**	**3.809**	**1.708**

Tabla 4.11.9 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**0.5**	**1**	**2**
Velocidad de Rx (Mbps)	**0.49**	**1**	**2**
Tramas Transmitidas	**426**	**851**	**1700**
Tramas Recibidas	**426**	**851**	**1700**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**8.183**	**6.65**	**2.25**

Tabla 4.11.10 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.



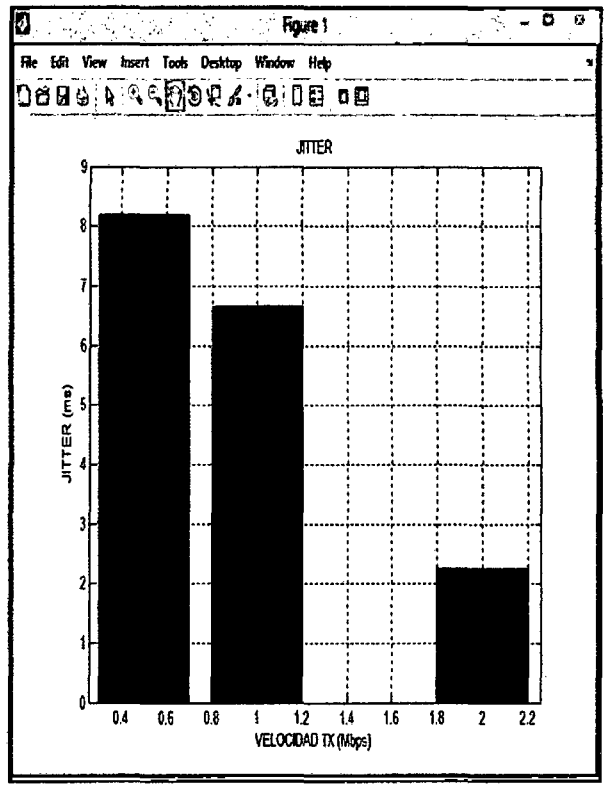


Fig. 4.11.22 Jitter vs. Tamaño de Trama

Fig. 4.11.23 Jitter vs. Velocidad Tx

En la figura 4.11.22 se observa los valores del Jitter obtenidos al enviar diferentes tamaños de paquete UDP como 750, 1125 y 1500 bytes utilizando una velocidad de Tx constante de 0.5 Mbps, se puede observar claramente que con una trama de 750 bytes se tiene un Jitter de 5.378 ms a diferencia de la trama de 1500 bytes en la cual se tiene un Jitter de 1.708 ms.

En la figura 4.11.23, se observa los valores del Jitter obtenidos al enviar paquetes UDP de 1470 bytes utilizando una velocidad de Tx que varía entre 0.5 Mbps, 1 Mbps y 2 Mbps sin que se pierdan paquetes en la red, concluyendo también que a mayor ancho de banda mucho mayor será el jitter y pérdidas de datagramas.

Medición de Jitter a 500 kbps:

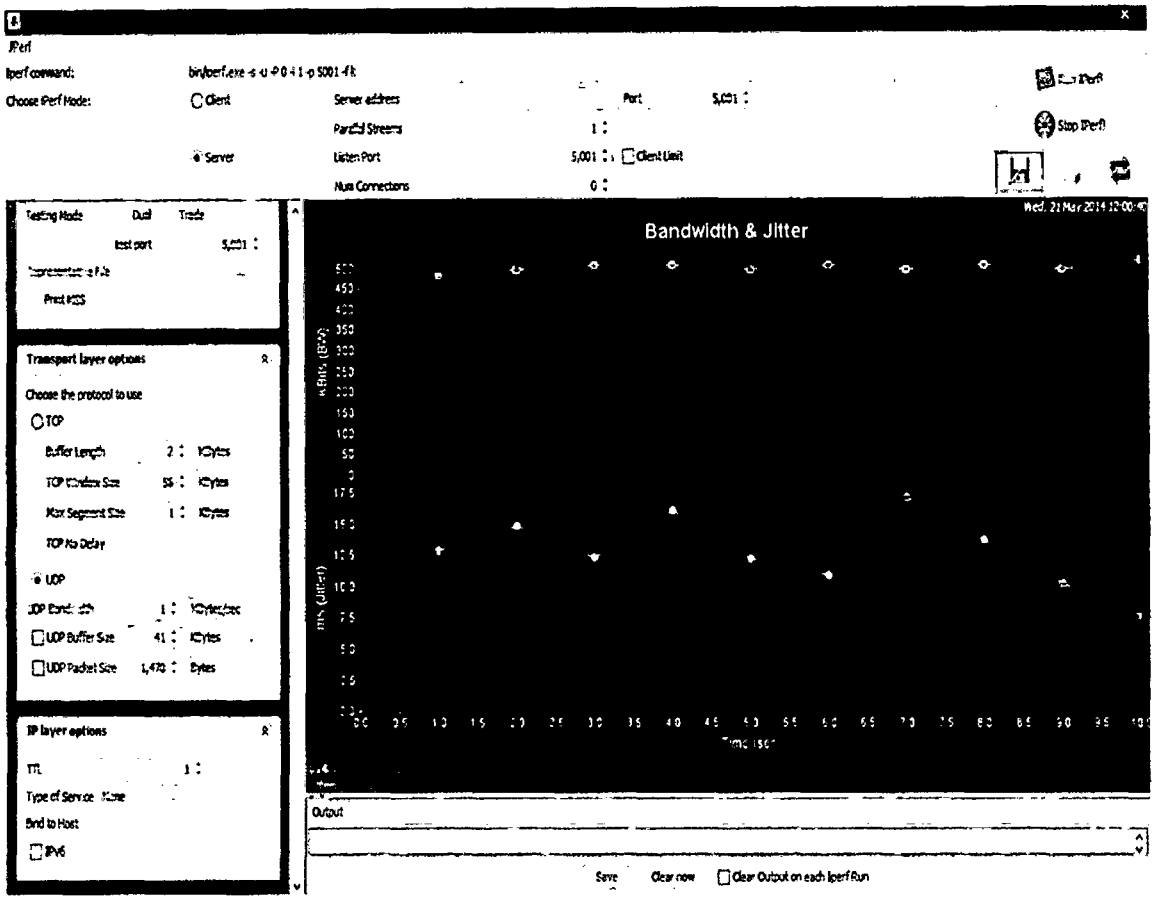


Fig. 4.11.24 Gráfica de Bandwidth y Jitter.

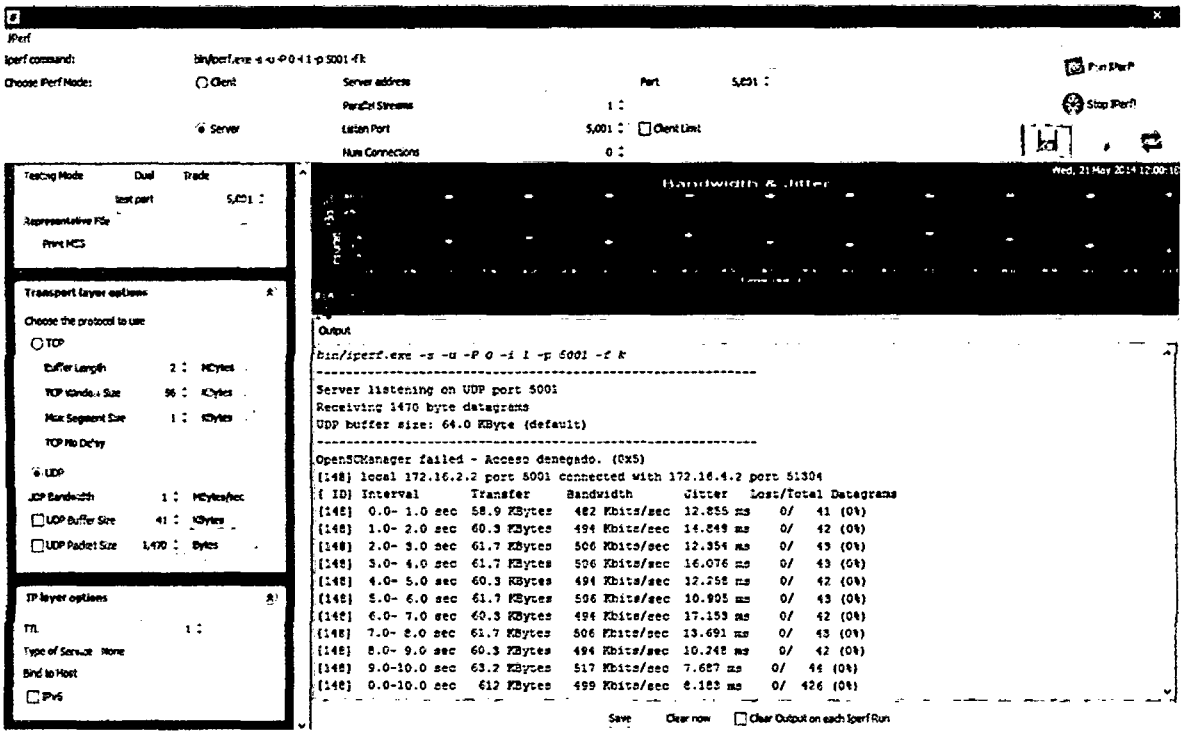


Fig. 4.11.25 Resultados al medir Throughput como servidor.

PASO 4: Captura de tráfico con Wireshark.

Capturar tráfico de paquetes en la interfaz s1/0 de R1.

- Captura de paquetes ICMP.

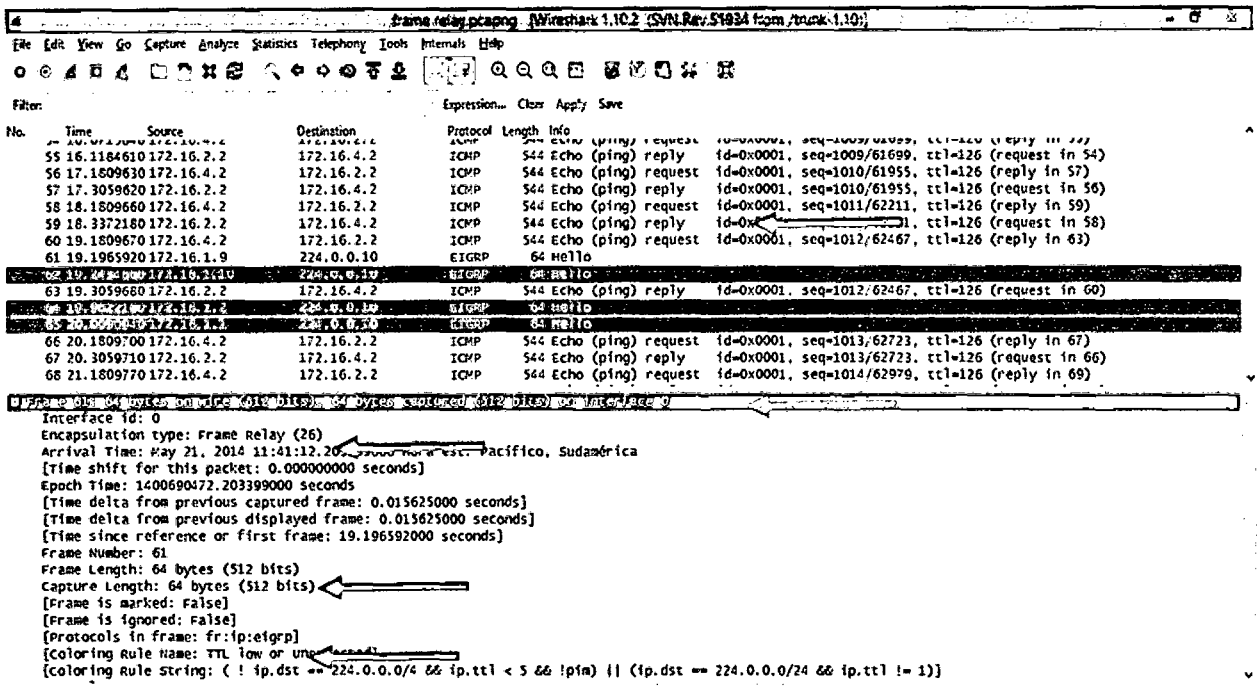


Fig. 4.11.26 Captura de paquetes ICMP con Wireshark.

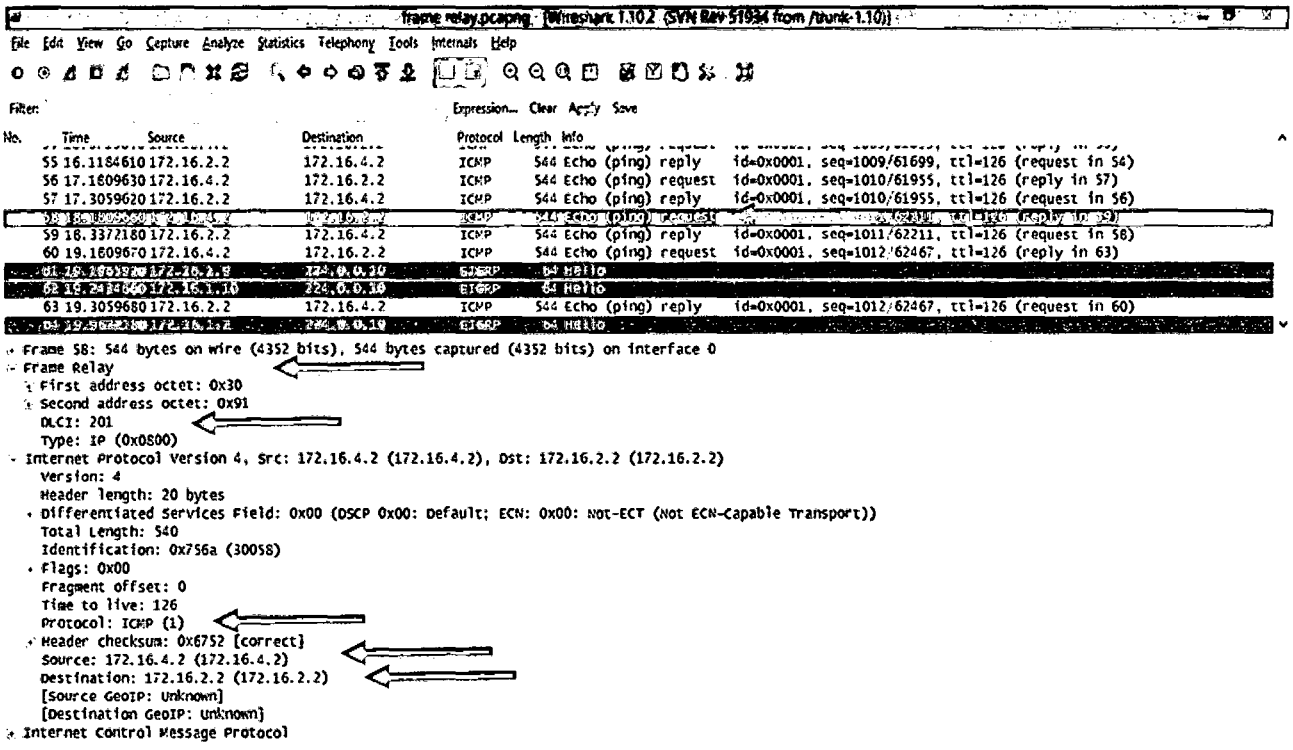


Fig. 4.11.27 Información detallada del origen y destino de paquetes.

- Protocolo de enrutamiento EIGRP.

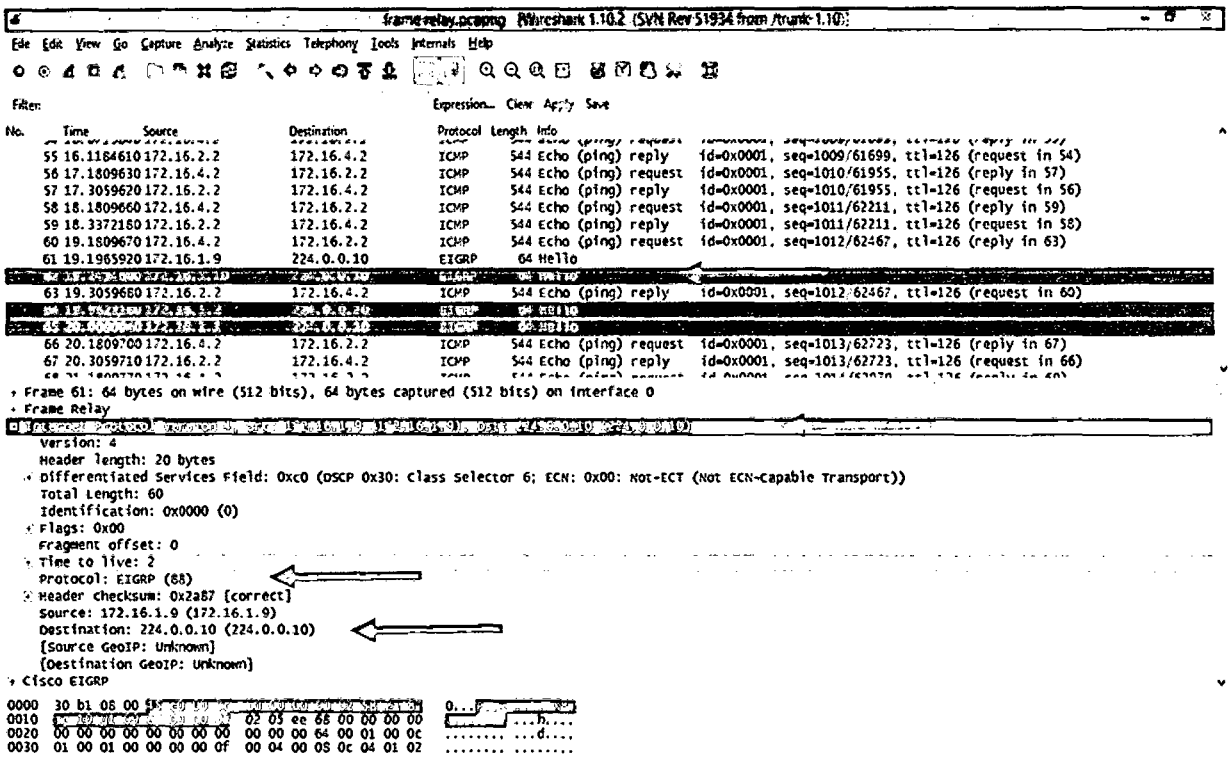


Fig. 4.11.28 Captura del protocolo EIGRP con Wireshark

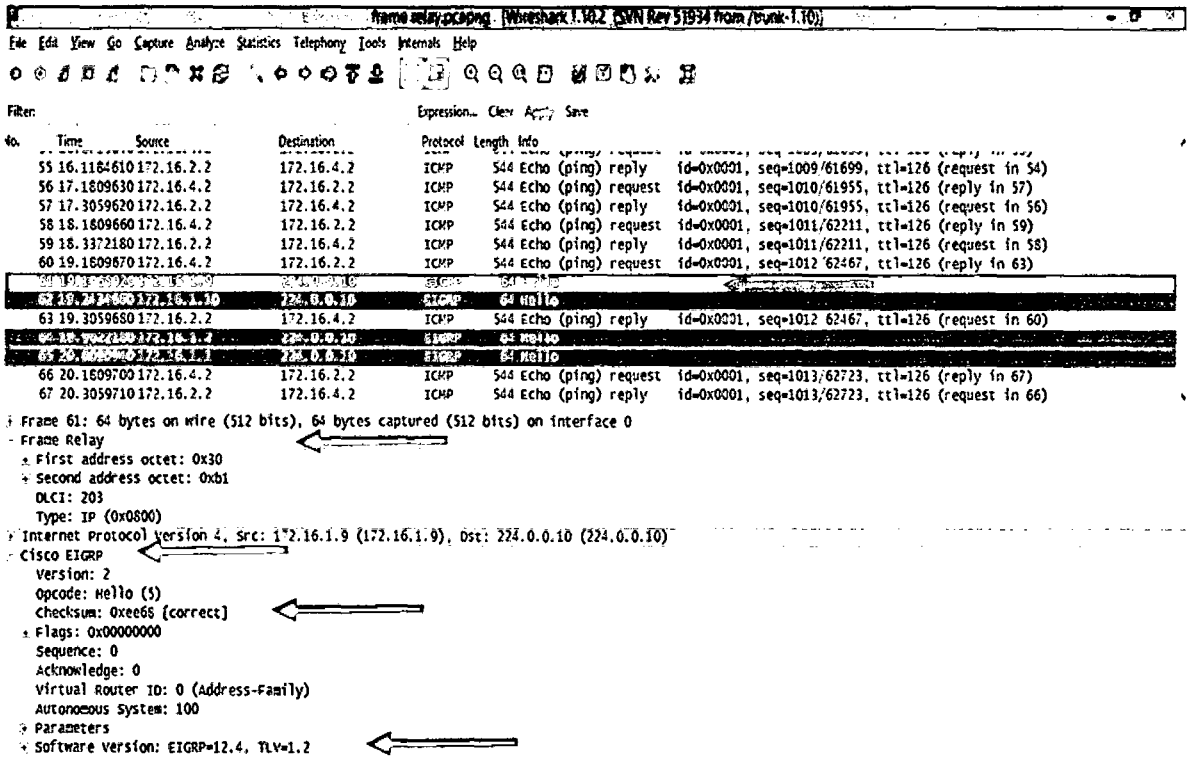


Fig. 4.11.29 Captura de la Encapsulacion Frame Relay con Wireshark.

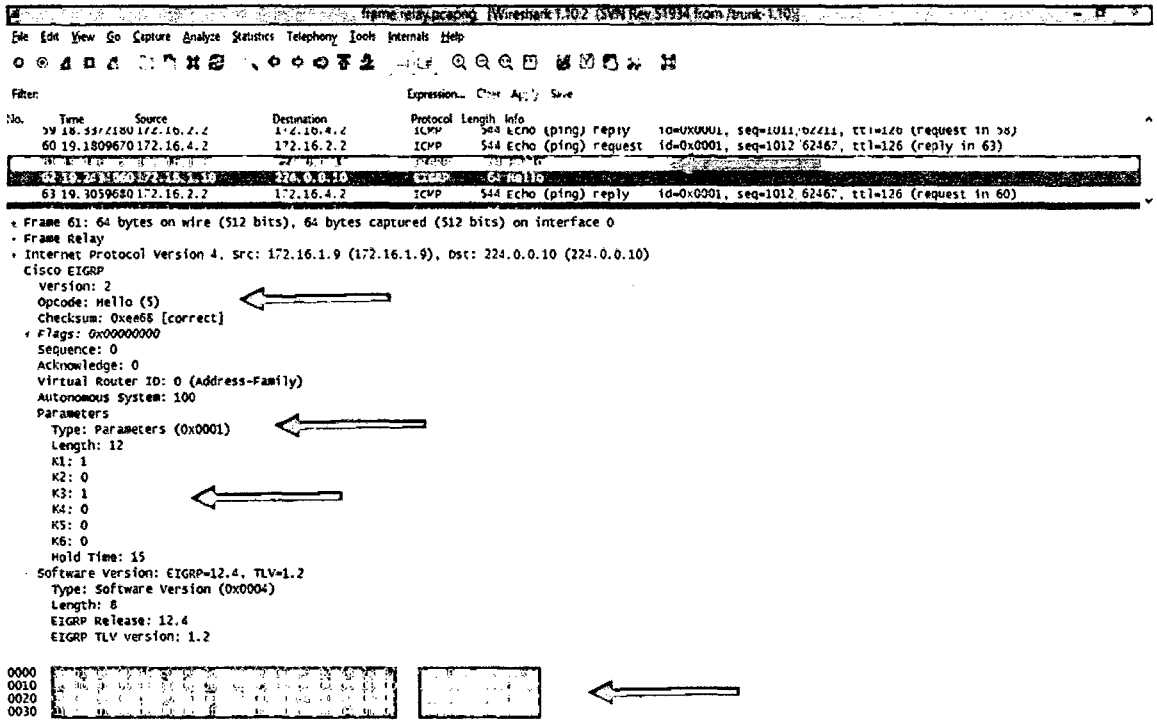


Fig. 4.11.30 Información detallada del protocolo EIGRP.

LABORATORIO 4.12: MPLS LDP

REVISIÓN TEÓRICA: Para la realización de esta práctica se deberá revisar conceptos de MPLS.

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet y GigabitEhernet.
- Configurar MPLS y el protocolo de distribución de etiquetas LDP.
- Configurar el enrutamiento OSPF.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **80.0.0.0/8** para obtener el direccionamiento IP usando VLSM para las interfaces seriales, además teniendo los siguientes requisitos:

LAN R5: 192.168.1.0/24
LAN R6: 192.168.1.0/24

DIAGRAMA DE TOPOLOGIA

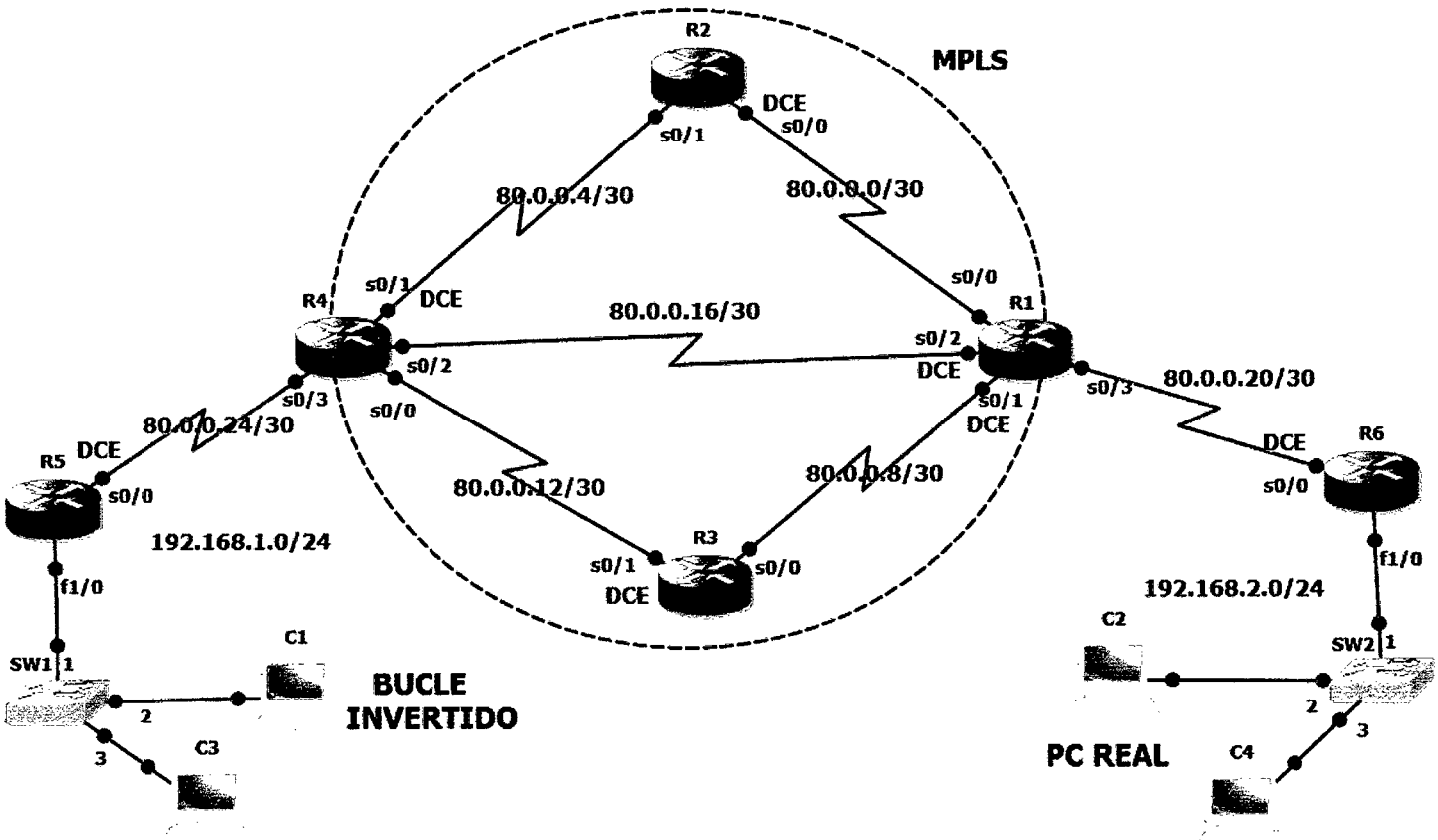


Fig. 4.12.1 Red Virtual en GNS3

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s0/0	80.0.0.1	255.255.255.252	No aplicable
	s0/1	80.0.0.9	255.255.255.252	No aplicable
	s0/2	80.0.0.17	255.255.255.252	No aplicable
	s0/3	80.0.0.21	255.255.255.252	No aplicable
R2	s0/0	80.0.0.2	255.255.255.252	No aplicable
	s0/1	80.0.0.5	255.255.255.252	No aplicable
R3	s0/0	80.0.0.10	255.255.255.252	No aplicable
	s0/1	80.0.0.13	255.255.255.252	No aplicable
R4	s0/0	80.0.0.14	255.255.255.252	No aplicable
	s0/1	80.0.0.6	255.255.255.252	No aplicable
	s0/2	80.0.0.18	255.255.255.252	No aplicable
	s0/3	80.0.0.25	255.255.255.252	No aplicable
R5	s0/0	80.0.0.26	255.255.255.252	No aplicable
	f1/0	192.168.1.1	255.255.255.0	No aplicable
R6	s0/0	80.0.0.22	255.255.255.252	No aplicable
	f1/0	192.168.2.1	255.255.255.0	No aplicable
C1	BUCLE INVERTIDO	192.168.1.2	255.255.255.0	192.168.1.1
C2	NIC	192.168.2.2	255.255.255.0	192.168.2.1
C3	VPCS	192.168.1.3	255.255.255.0	192.168.1.1
C4	VPCS	192.168.2.3	255.255.255.0	192.168.2.1

Tabla 4.12.1 Direccionamiento IP para las Redes

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET.

TAREA 4: CONFIGURAR OSPF.

R1:

R1(config)# **router ospf 1**

R1(config-router)# **network 80.0.0.0 0.0.0.3 area 0**

R1(config-router)# **network 80.0.0.8 0.0.0.3 area 0**

R1(config-router)# **network 80.0.0.16 0.0.0.3 area 0**

R1(config-router)# **network 80.0.0.20 0.0.0.3 area 0**

R1(config-router)# **exit**

NOTA: Seguir los mismos pasos para los demás routers, son sus respectivas redes.

TAREA 5: CONFIGURAR MPLS.

R1:

R1(config)# **interface serial 0/0**

R1(config-if)# **mpls ip**

R1(config-if)# **exit**

R1(config)# **interface serial 0/1**

R1(config-if)# **mpls ip**

R1(config-if)# **exit**

R1(config)# **interface serial 0/2**

R1(config-if)# **mpls ip**

R1(config-if)# **exit**

Configurar rango de etiquetas MPLS entre 20-200

R1(config)# **mpls label range 20 200**

Configurar envio de MPLS Hello cada 2 segundos

R1(config)# **mpls ldp discovery hello internal 2**

Configurar el tiempo de mantenimiento de MPLS Hello cada 10 segundos.

R1(config)# **mpls ldp discovery hello holdtime 10**

Copiar TTL de los paquetes IP en las etiquetas de cada router.

R1(config)# **mpls ip propagate-ttl**

TAREA 6: CONFIGURAR LOS EQUIPOS DE HOST.

BUCLE INVERTIDO

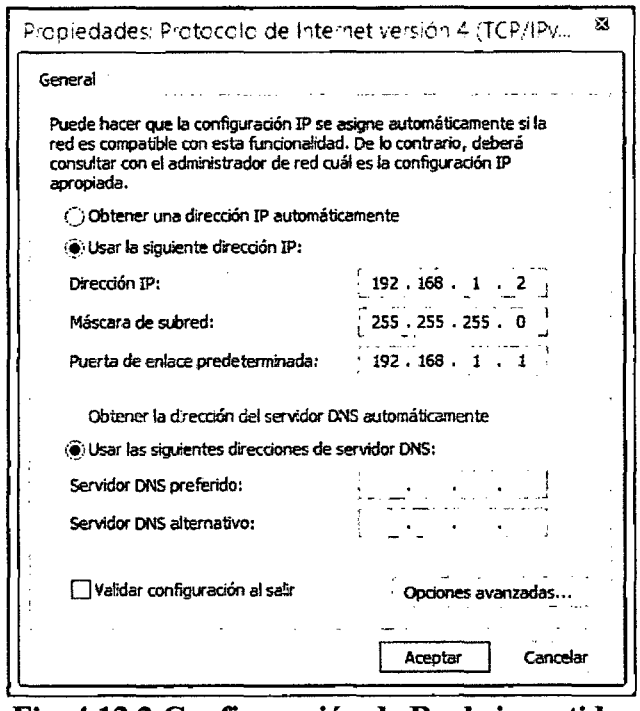


Fig. 4.12.2 Configuración de Bucle invertido.

VPCS

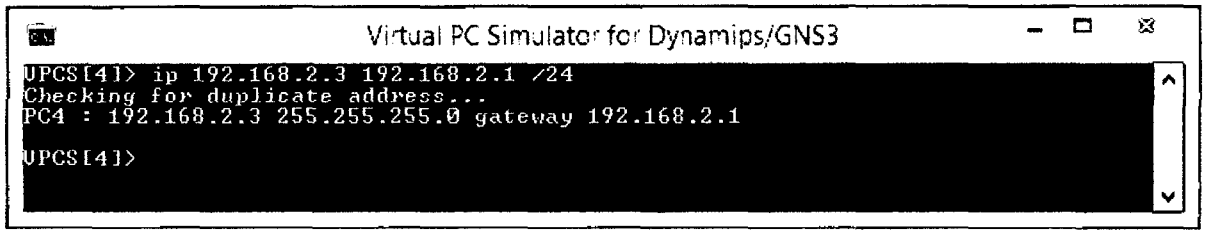


Fig. 4.12.3 Dirección IP de las VPCS.

NOTA: Seguir los mismos pasos para asignar IPs a los demás host.

TAREA 7: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

PASO 1: Verificar configuraciones.

R1#show mpls forwarding-table

Muestra la tabla de forwarding de MPLS. Si se indica una IP, muestra el detalle para la entrada correspondiente al bloque que contiene esa IP. Si se indica la palabra "detail", nos da más información.

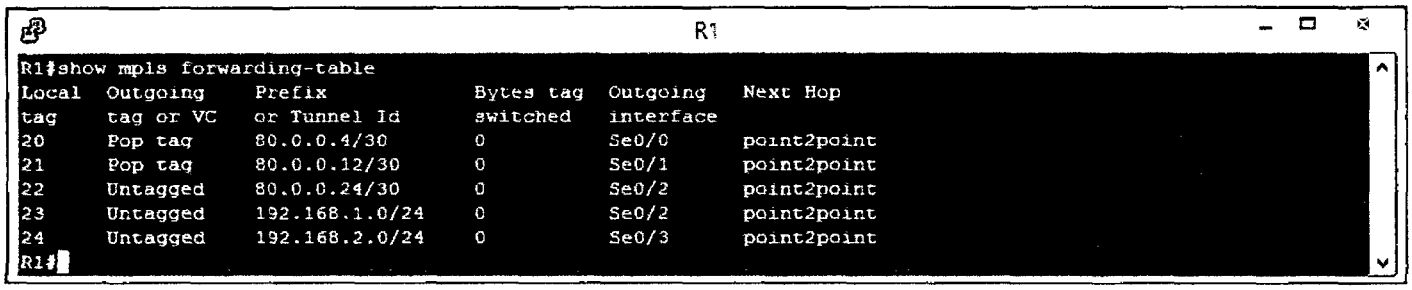


Fig. 4.12.4 Tabla mpls forwarding de R1.

R1#show mpls interfaces

Muestra información de MPLS de las distintas interfaces (protocolo de etiquetas, si está corriendo MPLS, etc). Con la palabra opcional "detail", muestra más información para cada interfaz (MTU, etc)

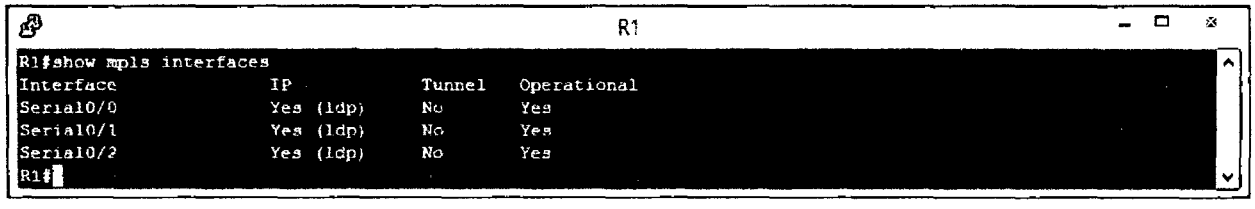


Fig. 4.12.5 Tabla mpls interfaces de R1.

R1#show mpls ldp neighbor

Muestra información de los vecinos LDP (Identidad, datos de la conexión TCP, IPs asociadas al vecino, etc.)

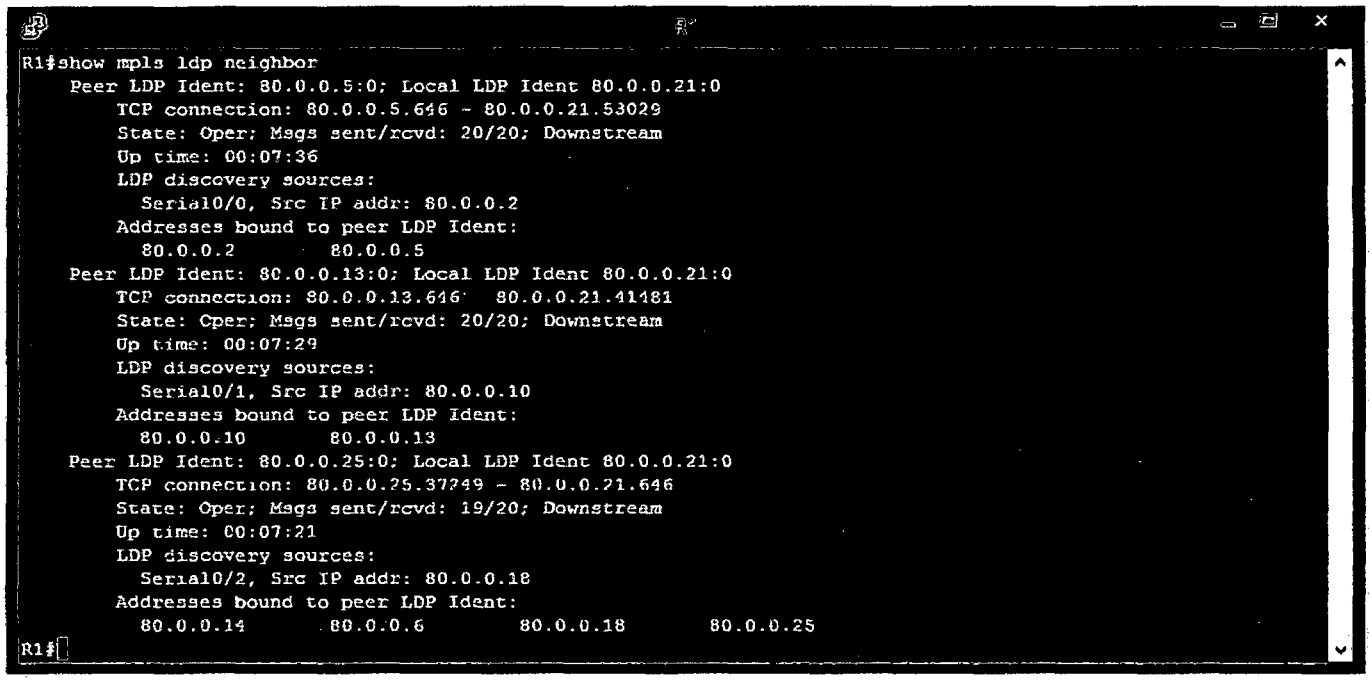


Fig. 4.12.6 Tabla mpls ldp neigborg en R1.

PASO 2: Utilice el comando ping para probar la conectividad entre los routers que no están directamente conectados y también la conectividad entre host.

PING ENTRE ROUTERS

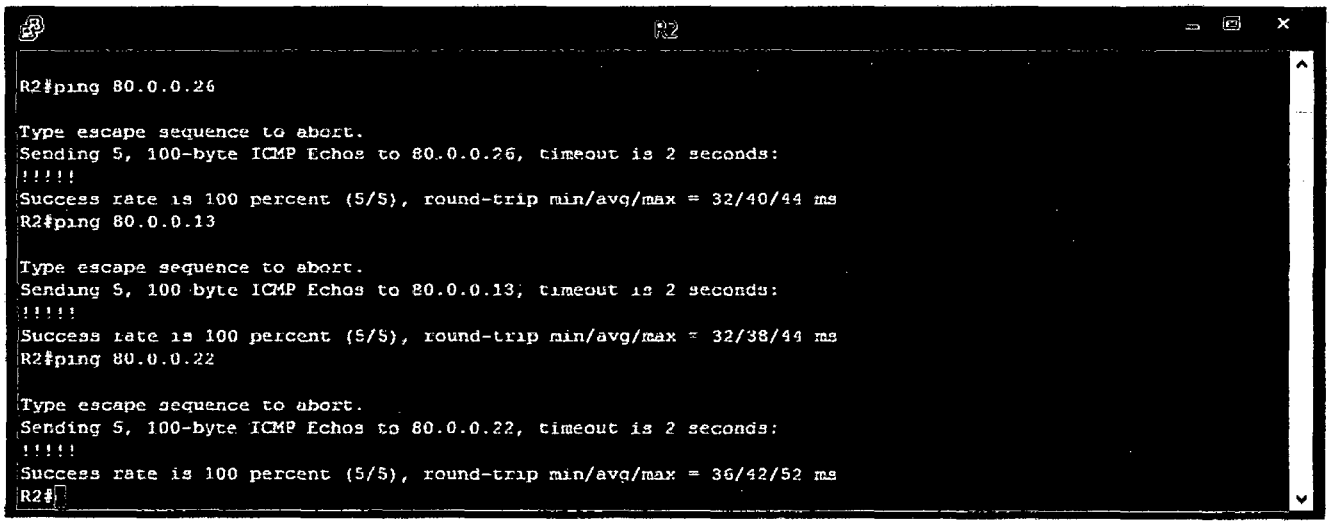


Fig. 4.12.7 Comprobación de conectividad entre routers.

PING ENTRE HOST

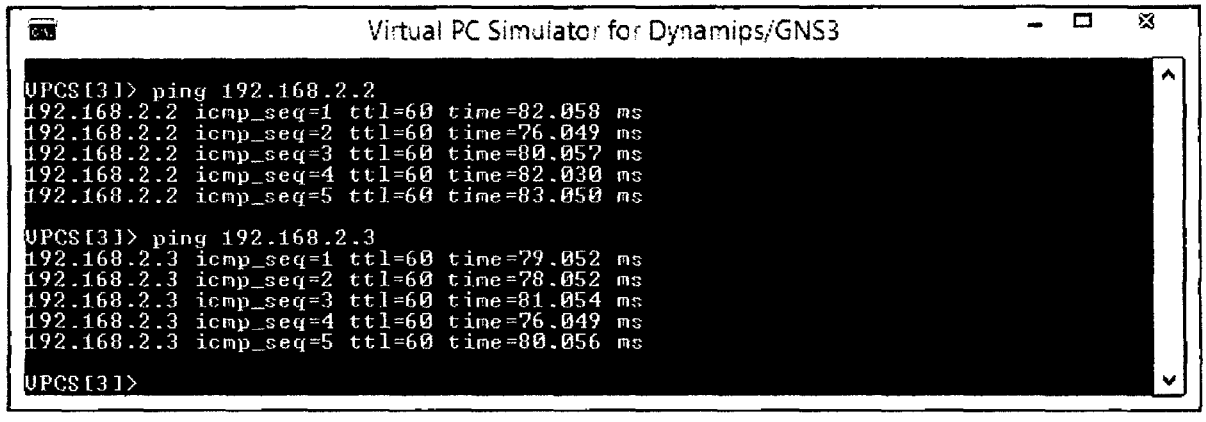


Fig. 4.12.8 Comprobación de conectividad entre VPCS.

NOTA: Realizar las pruebas faltantes.

TAREA 8: ANALIS DEL TRAFICO DE PAQUETES

PASO 1: Medición de la Latencia

Para la medición de la latencia se realizó 10 muestras sucesivas de 100 ping desde el C2 (Bucle invertido) hacia la PC REAL considerando un tamaño de trama de 64, 512 y 1518 bytes como se especifica en el RFC 2544.

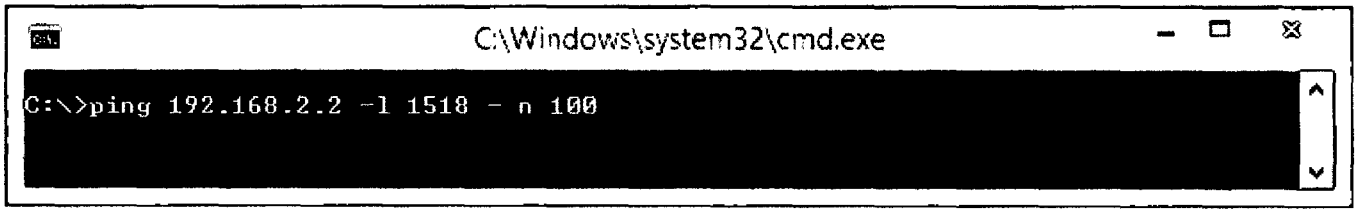


Fig. 4.12.9 Forma de medición de la latencia.

En la Figura 4.12.9 se puede observar el envío de 100 ping con una trama de 1518 hacia la dirección 192.168.2.2

En las Tablas posteriores se detallan los valores de la Latencia que se ha obtenido una vez realizadas todas las muestras.

LATENCIA											
Tamaño de Trama (bytes)	64										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	59	51	65	73	55	51	73	57	52	63	59.9
Tiempo Máximo (ms)	82	83	85	82	83	83	83	83	83	82	82.9
Tiempo Promedio (ms)	74	74	76	77	74	72	76	72	74	75	74.4

Tabla 4.12.2 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	512										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	71	72	71	74	73	71	72	71	72	71	71.8
Tiempo Máximo (ms)	81	84	83	85	85	83	83	82	83	82	83.1
Tiempo Promedio (ms)	76	76	77	78	77	76	76	76	77	76	76.5

Tabla 4.12.3 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1518										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	85	84	91	91	84	73	87	81	91	93	86
Tiempo Máximo (ms)	113	108	112	116	122	107	241	112	133	115	127.9
Tiempo Promedio (ms)	99	97	100	99	100	96	105	98	101	100	99.5

Tabla 4.12.4 Datos obtenidos para una trama de 1518 bytes.

LATENCIA			
Tamaño de Trama (bytes)	**64**	**512**	**1518**
Tiempo Mínimo (ms)	**59.9**	**71.8**	**86**
Tiempo Máximo (ms)	**82.9**	**83.1**	**127.9**
Tiempo Promedio (ms)	**74.4**	**76.5**	**99.5**

Tabla 4.12.5 Comparación de datos obtenidos de las diferentes tramas.

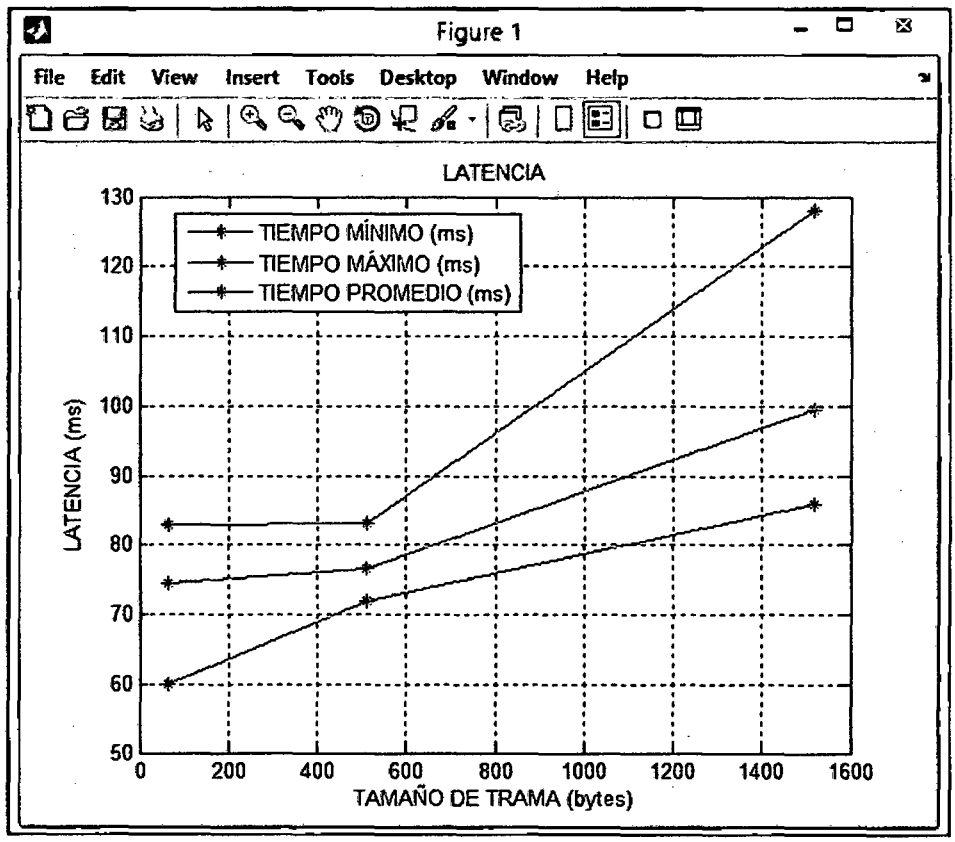


Fig. 4.12.10 Datos representados gráficamente de la variación de la latencia.

De acuerdo con los datos obtenidos, se puede observar claramente que los valores mínimo (color azul), máximo (color rojo) y promedio (color verde) de la latencia de la red se incrementan conforme se envía una trama de longitud mayor, en este caso con la trama de 1518 bytes se obtiene una latencia promedio de 99.5 ms a diferencia de una trama de 64 bytes con 74.4 ms.

PASO 2: Medición del Throughput

Para la medición del Throughput y Jitter se envió una cantidad de tramas a velocidades diferentes durante 20 segundos, hasta encontrar la máxima cantidad de tramas recibidas sin que se produzcan perdidas de las mismas en el router y PC REAL. Como se utilizó Jperf el cliente será el encargado de enviar los paquetes y el servidor los recibirá, indicando la cantidad de paquetes que llegaron correctamente considerando un tamaño del paquete UDP de 750, 1125, 1500 y 1470 (default) bytes, tal como se especifica en el RFC 768.

Configuración del Jperf como servidor con UDP Packet Size 750 Bytes

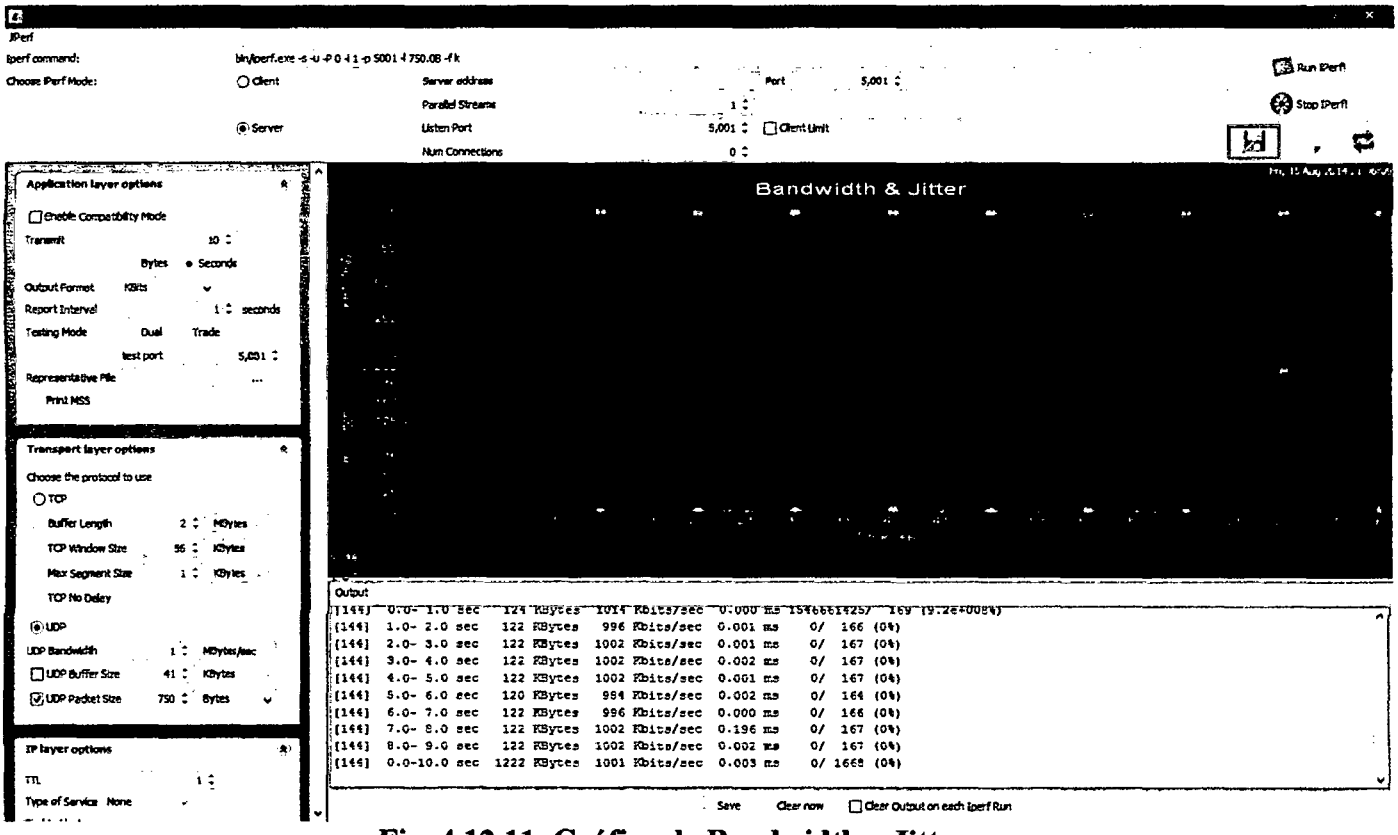


Fig. 4.12.11 Gráfica de Bandwidth y Jitter.

```
bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -l 750.0B -f k
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 750 byte datagrams
UDP buffer size: 64.0 KByte (default)
------------------------------------------------------------
OpenSCManager failed - Acceso denegado. (0x5)
[144] local 192.168.2.2 port 5001 connected with 169.254.35.253 port 63236
[ ID] Interval       Transfer     Bandwidth        Jitter   Lost/Total Datagrams
[144]  0.0- 1.0 sec   124 KBytes  1014 Kbits/sec  0.000 ms 1546661425/  169 (9.2e+008%)
[144]  1.0- 2.0 sec   122 KBytes   996 Kbits/sec  0.001 ms    0/  166 (0%)
[144]  2.0- 3.0 sec   122 KBytes  1002 Kbits/sec  0.001 ms    0/  167 (0%)
[144]  3.0- 4.0 sec   122 KBytes  1002 Kbits/sec  0.002 ms    0/  167 (0%)
[144]  4.0- 5.0 sec   122 KBytes  1002 Kbits/sec  0.001 ms    0/  167 (0%)
[144]  5.0- 6.0 sec   120 KBytes   984 Kbits/sec  0.002 ms    0/  164 (0%)
[144]  6.0- 7.0 sec   122 KBytes   996 Kbits/sec  0.000 ms    0/  166 (0%)
[144]  7.0- 8.0 sec   122 KBytes  1002 Kbits/sec  0.196 ms    0/  167 (0%)
[144]  8.0- 9.0 sec   122 KBytes  1002 Kbits/sec  0.002 ms    0/  167 (0%)
[144]  0.0-10.0 sec  1222 KBytes  1001 Kbits/sec  0.003 ms    0/ 1668 (0%)
```

Fig. 4.12.12 Resultados al medir como servidor.

Configuración del Jperf como cliente con UDP Bandwidth de 1 Mbps y UDP Packet Size de 750 Bytes.

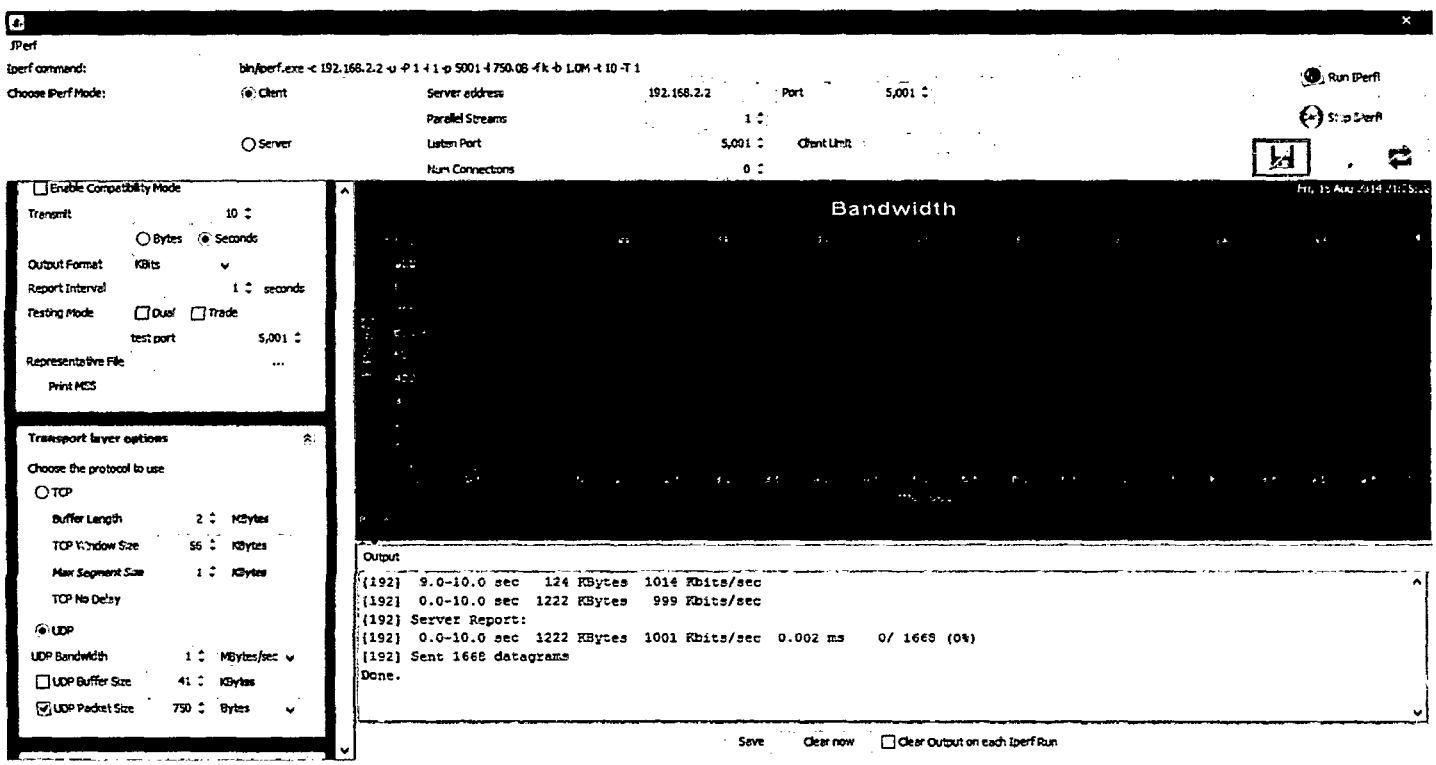


Fig. 4.12.13 Resultados del Jperf como Cliente.

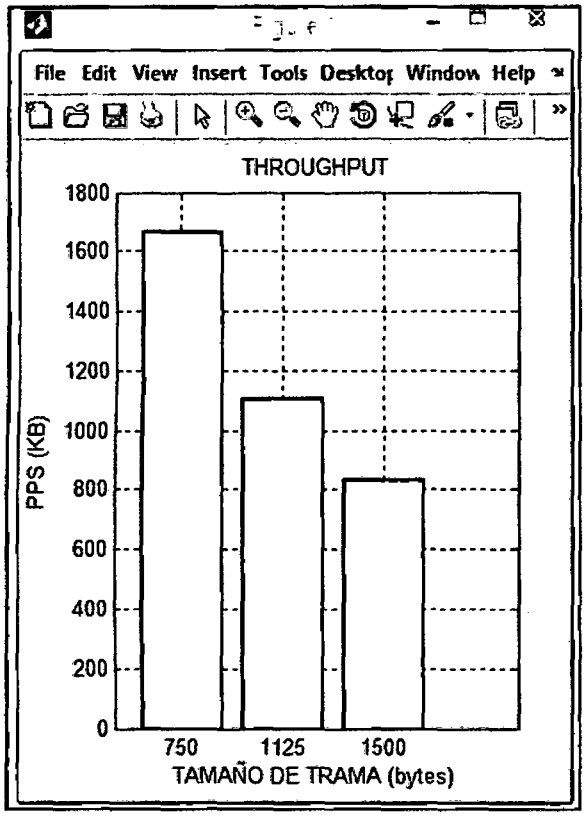
En las siguientes Tablas se detalla los valores del Throughput obtenidos una vez realizada todas las muestras.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**1**	**1**	**1**
Velocidad de Rx (Mbps)	**1**	**1**	**1**
Tramas Transmitidas	**1668**	**1111**	**834**
Tramas Recibidas	**1668**	**1111**	**834**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**166.8**	**111.1**	**83.4**

Tabla 4.12.6 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**0.5**	**0.8**	**1**
Velocidad de Rx (Mbps)	**0.5**	**0.8**	**1**
Tramas Transmitidas	**426**	**681**	**851**
Tramas Recibidas	**426**	**681**	**851**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**42.6**	**68.1**	**85.1**

Tabla 4.12.7 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.



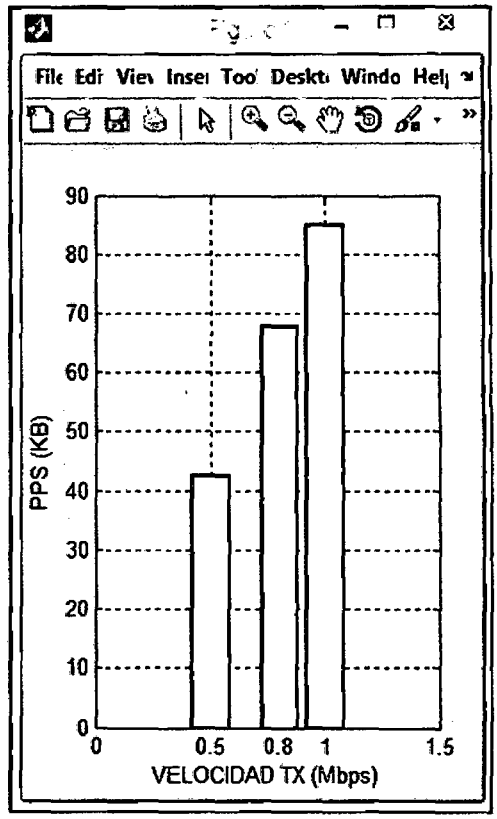


Fig. 4.12.14 PPS vs. Tamaño de Trama.

Fig. 4.12.15 PPS vs. Velocidad Tx.

En la figura 4.12.14, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 750 bytes, 1125 bytes y 1500 bytes los cuales han utilizado una velocidad de Tx constante de 1 Mbps, en la gráfica se puede observar claramente que al enviar una trama de 750 bytes se envía 1666 pps, con una trama de 1125 se envía 1111 pps y con una trama de 1500 se envía 834 pps.

Mientras en la figura 4.12.15, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 1470 bytes los cuales han utilizado una velocidad de Tx variada de: 0.5 Mbps, 0.8 Mbps y 1 Mbps, sin que se produzcan perdidas en el envío, como los datos que se muestran en la tabla 4.12.7.

PASO 3: Medición del Jitter

Para la medición se envió datos UDP de longitud variable a velocidades diferentes de Throughput obtenida anteriormente durante 20 segundos. Como se utilizó anteriormente Jperf el cliente será el encargado de enviar los datos y el servidor los recibirá, indicando los valores de Jitter obtenidos durante la transmisión de los datos.

Configuración del Jperf como servidor con UDP Packet Size por defecto.

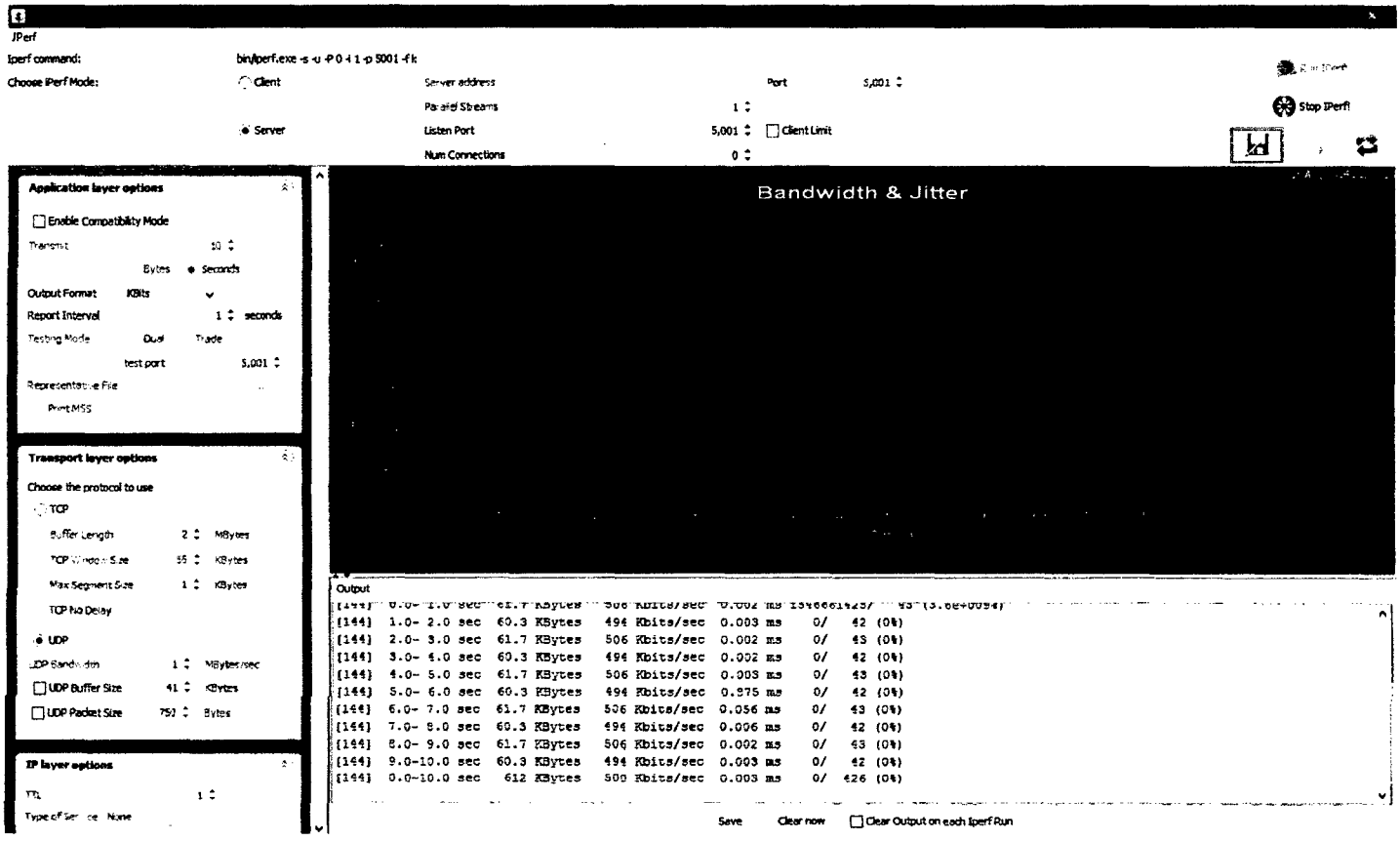


Fig. 4.12.16 Gráfica de Bandwidth y Jitter.

```
bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -f k
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 64.0 KByte (default)
------------------------------------------------------------
OpenSCManager failed - Acceso denegado. (0x5)
[144] local 192.168.2.2 port 5001 connected with 169.254.35.253 port 55418
[ ID] Interval       Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[144]  0.0- 1.0 sec  61.7 KBytes   506 Kbits/sec  0.002 ms 1546661425/   43 (3.6e+009%)
[144]  1.0- 2.0 sec  60.3 KBytes   494 Kbits/sec  0.003 ms    0/   42 (0%)
[144]  2.0- 3.0 sec  61.7 KBytes   506 Kbits/sec  0.002 ms    0/   43 (0%)
[144]  3.0- 4.0 sec  60.3 KBytes   494 Kbits/sec  0.002 ms    0/   42 (0%)
[144]  4.0- 5.0 sec  61.7 KBytes   506 Kbits/sec  0.003 ms    0/   43 (0%)
[144]  5.0- 6.0 sec  60.3 KBytes   494 Kbits/sec  0.875 ms    0/   42 (0%)
[144]  6.0- 7.0 sec  61.7 KBytes   506 Kbits/sec  0.056 ms    0/   43 (0%)
[144]  7.0- 8.0 sec  60.3 KBytes   494 Kbits/sec  0.006 ms    0/   42 (0%)
[144]  8.0- 9.0 sec  61.7 KBytes   506 Kbits/sec  0.002 ms    0/   43 (0%)
[144]  9.0-10.0 sec  60.3 KBytes   494 Kbits/sec  0.003 ms    0/   42 (0%)
[144]  0.0-10.0 sec   612 KBytes   500 Kbits/sec  0.003 ms    0/  426 (0%)
```

Fig. 4.12.17 Resultados al medir como servidor.

En las siguientes Tablas se detalla los valores del Jitter obtenidos una vez realizada todas las muestras.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**1**	**1**	**1**
Velocidad de Rx (Mbps)	**1**	**1**	**1**
Tramas Transmitidas	**1668**	**1111**	**834**
Tramas Recibidas	**1668**	**1111**	**834**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**0.003**	**0.117**	**0.310**

Tabla 4.12.8 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**0.5**	**0.8**	**1**
Velocidad de Rx (Mbps)	**0.5**	**0.8**	**1**
Tramas Transmitidas	**426**	**681**	**851**
Tramas Recibidas	**426**	**681**	**851**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**0.003**	**0.158**	**0.297**

Tabla 4.12.9 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

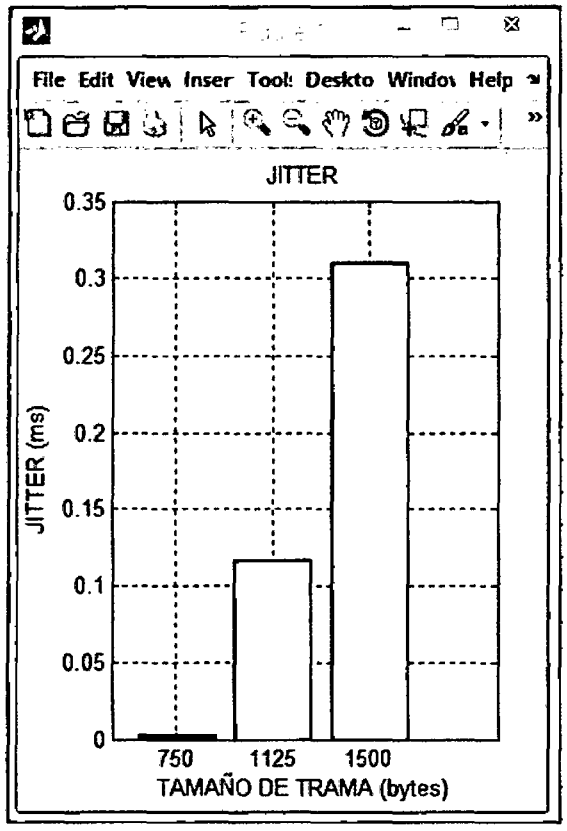


Fig. 4.12.18 Jitter vs. Tamaño de Trama Tx

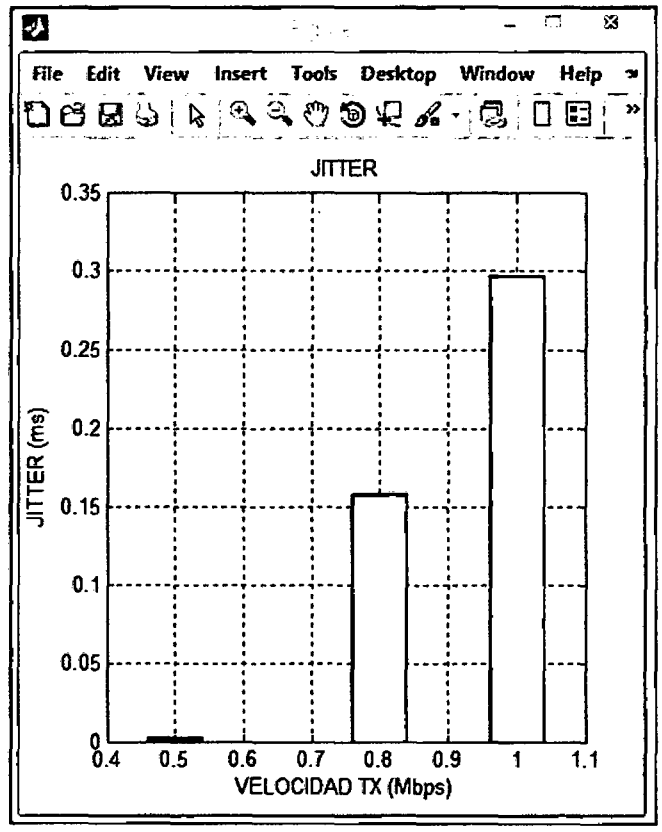


Fig. 4.12.19 Jitter vs. Velocidad

En la figura 4.12.18 se observa los valores del Jitter obtenidos al enviar diferentes tamaños de paquete UDP como 750, 1125 y 1500 bytes utilizando una velocidad de Tx constante de 1 Mbps, se puede observar claramente que con una trama de 750 bytes se tiene un Jitter de 0.003 ms a diferencia de la trama de 1500 bytes en la cual se tiene un Jitter de 0.310 ms.

En la figura 4.12.19, se observa los valores del Jitter obtenidos al enviar paquetes UDP de 1470 bytes utilizando una velocidad de Tx que varía de: 0.5 Mbps, 0.8 Mbps y 1 Mbps, sin que se pierdan paquetes en la red.

PASO 4: Captura de tráfico con Wireshark.

Capturar tráfico de datos en la interface serial 0/1 de R4.

- Captura de paquetes LDP

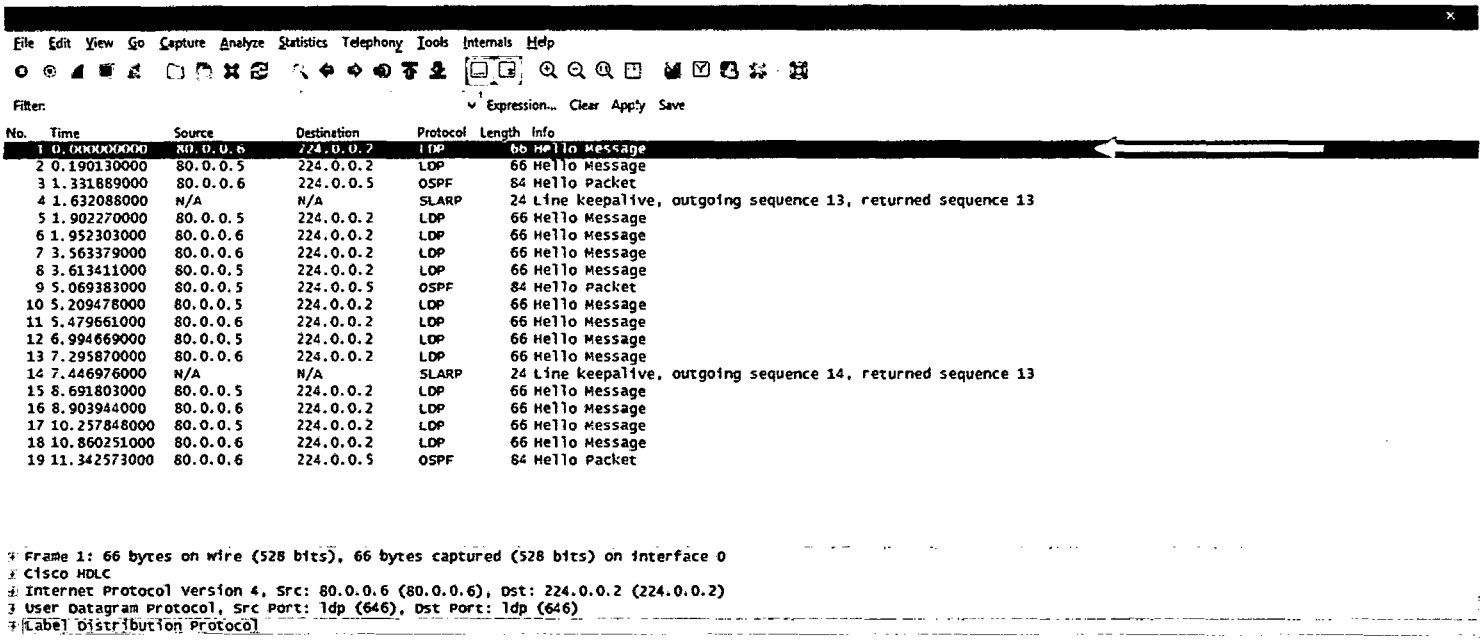


Fig. 4.12.20 Captura de paquete LDP con Wireshark.

Información más detallada sobre el paquete LDP.

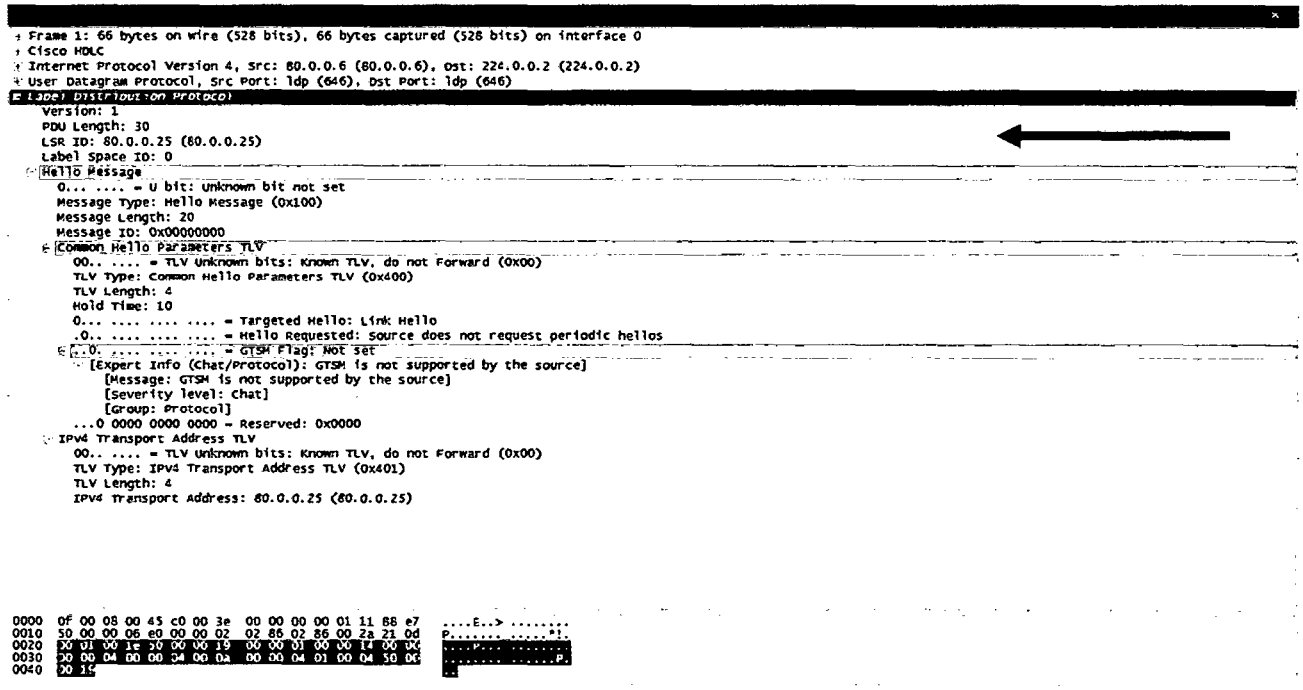


Fig. 4.12.21 Información detallada del paquete LDP.

- Captura de paquetes HELLO OSPF.

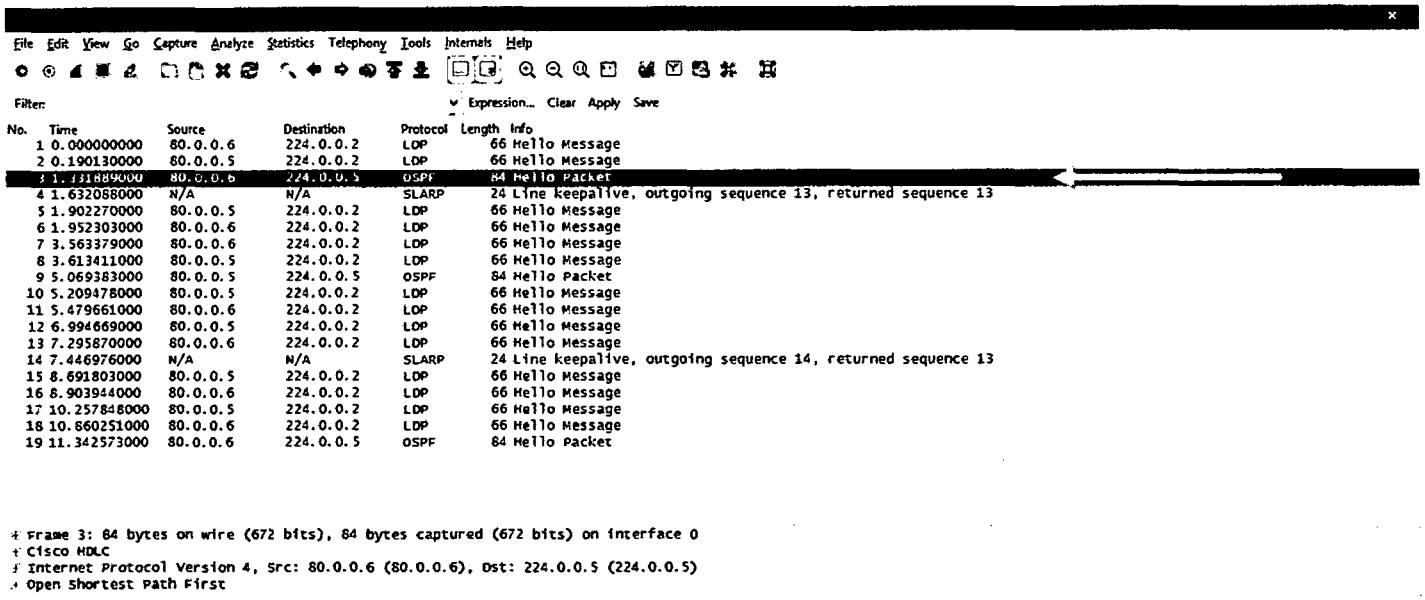


Fig. 4.12.22 Captura de paquete HELLO OSPF con Wireshark.

Información más detallada sobre el paquete HELLO.

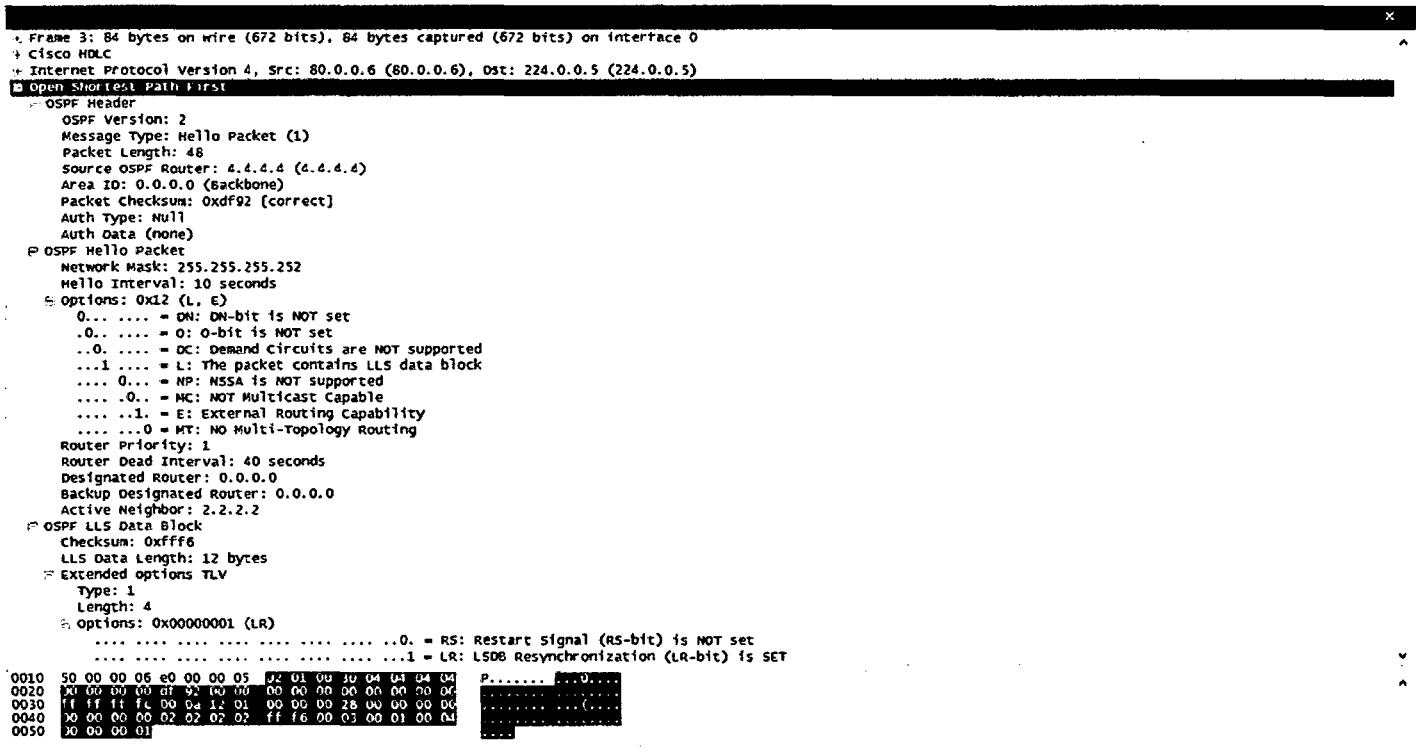


Fig. 4.12.23 Información detallada del paquete HELLO OSPF.

Capturar tráfico de datos en la interface serial 0/2 de R1.

- Captura de paquetes ICMP.

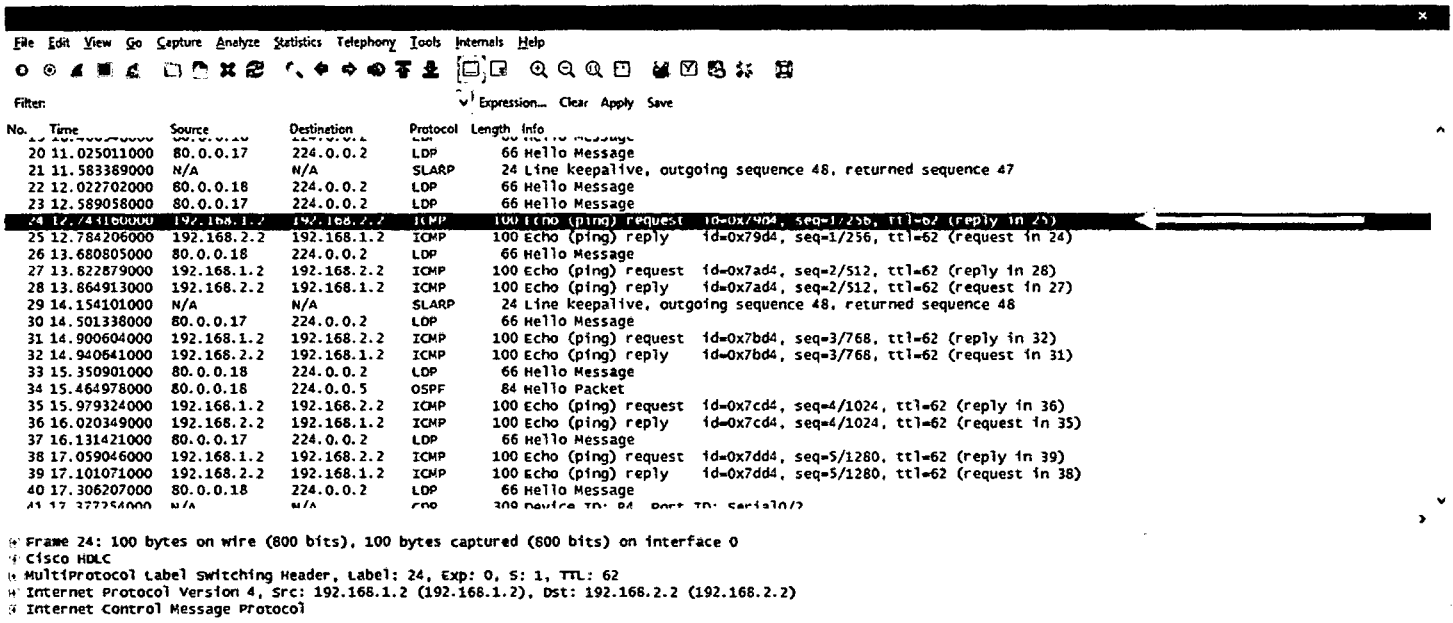


Fig. 4.12.24 Captura de paquete ICMP con Wireshark.

Información más detallada sobre el paquete ICMP.

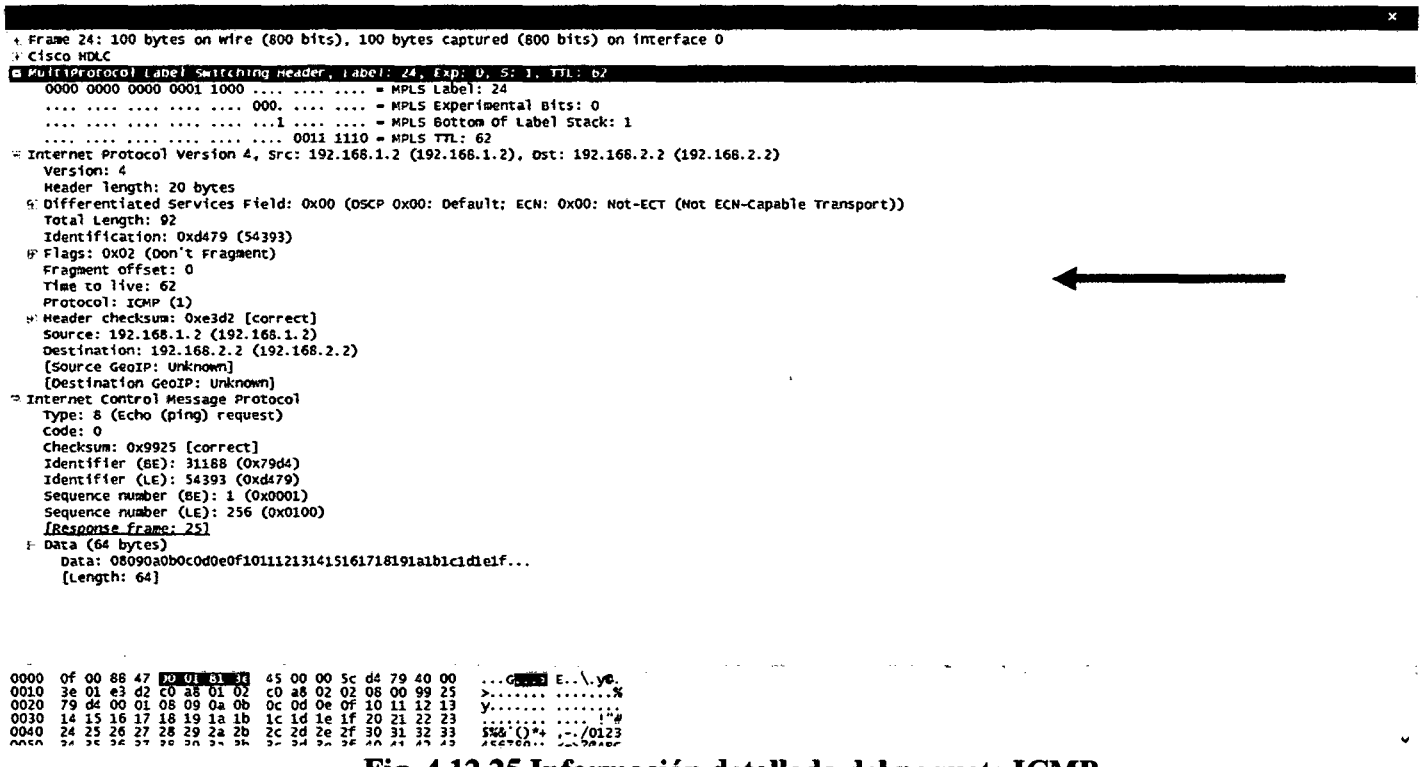


Fig. 4.12.25 Información detallada del paquete ICMP.

- Captura de paquetes Traceroute

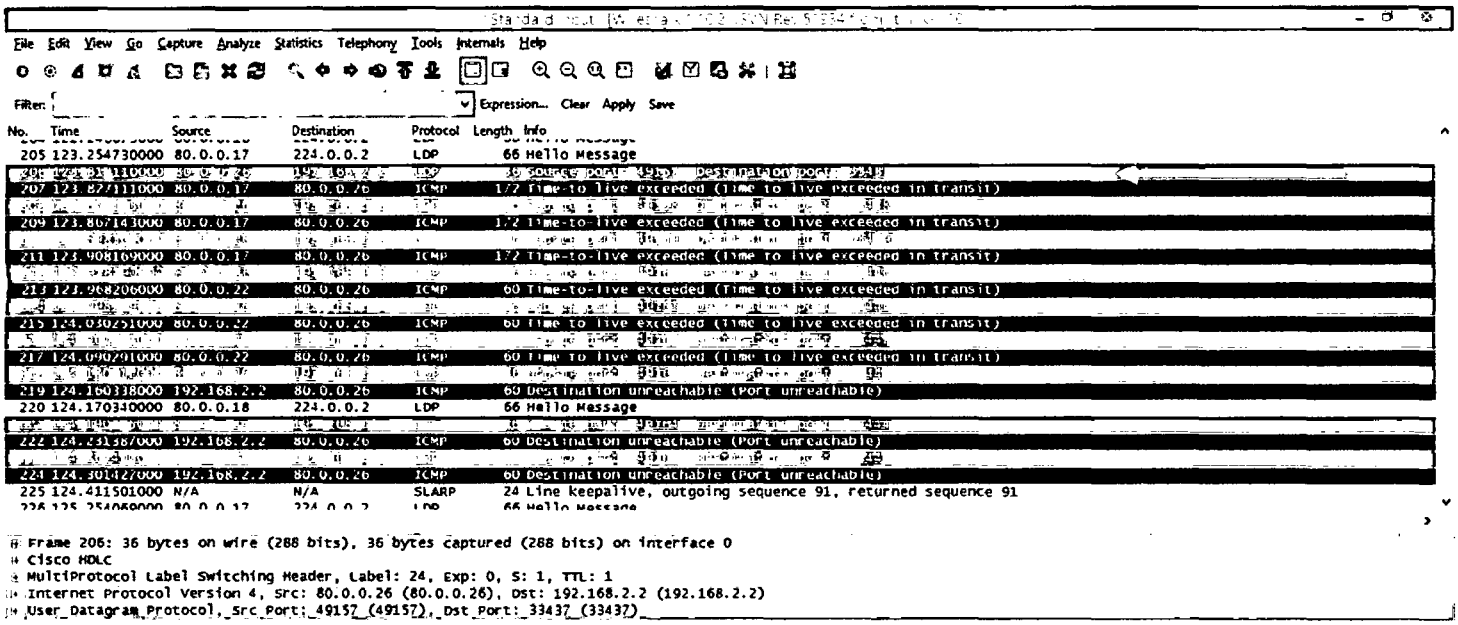


Fig. 4.12.26 Captura de paquete Traceroute con Wireshark.

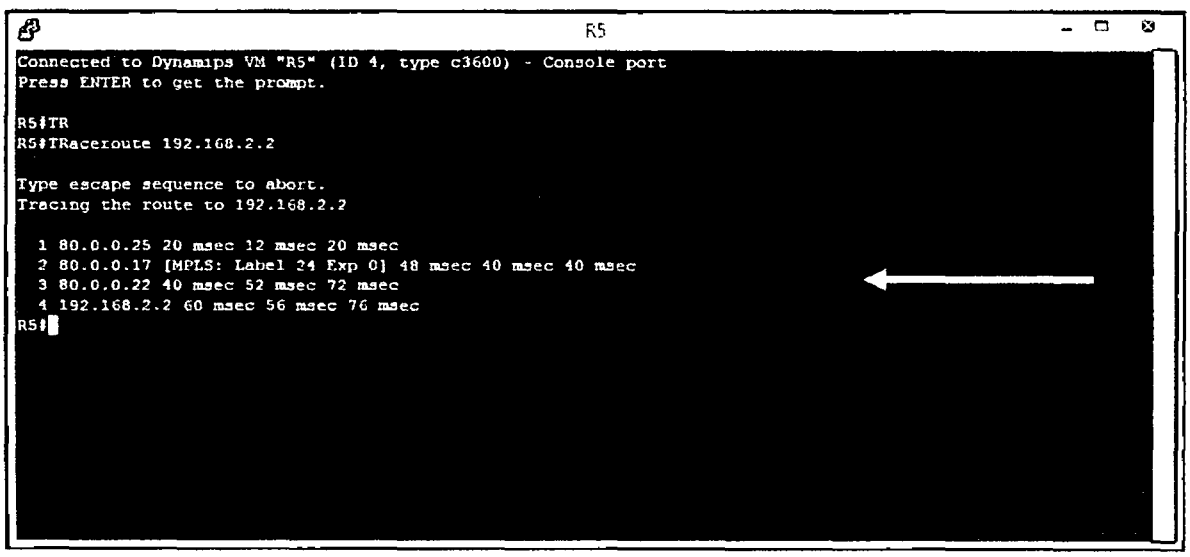


Fig. 4.12.27 Información detallada del paquete Traceroute.

- Captura de paquetes Telnet

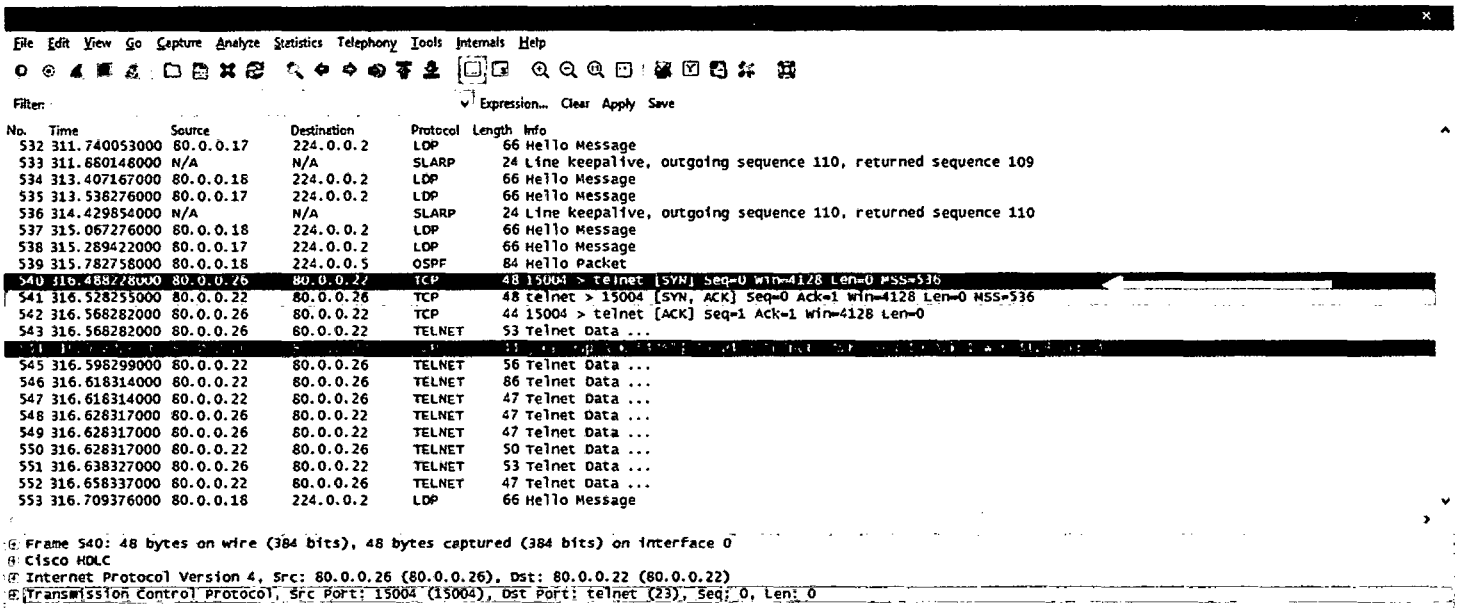


Fig. 4.12.28 Captura de paquete Telnet con Wireshark.

LABORATORIO 4.13: CONFIGURACION BASICA DE DHCP Y NAT

REVISIÓN TEÓRICA: Para la realización de esta práctica se deberá revisar conceptos de fundamentales de DHCP y NAT.

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, el usuario podrá:

- Preparar la red
- Realizar las configuraciones básicas del router
- Configurar un servidor de DHCP del IOS de Cisco
- Configurar el enrutamiento estático y por defecto
- Configurar NAT estática
- Configurar NAT dinámica con un conjunto de direcciones
- Configurar la sobrecarga de NAT
- Probar la conectividad.
- Análisis de tráfico de paquetes.

ESCENARIO:

En esta actividad de laboratorio, se configurarán los servicios IP de DHCP y NAT. Un router es el servidor de DHCP. Los otros routers envían solicitudes de DHCP al servidor. Además, se establecerán las de NAT estática y dinámica, incluida la sobrecarga de NAT. El usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **172.16.0.0/16** para obtener el direccionamiento IP usando VLSM, teniendo los siguientes requisitos:

LAN 1 de R3: 186 direcciones IP de host.
LAN 2 de R1: 250 direcciones IP de host.
LAN 3 de R2: 254 direcciones IP de host.

Considerando también las redes que hay entre router y router (enlaces WAN).

Después de completar la configuración pruebe la conectividad entre los dispositivos de la red y finalmente analizará el tráfico de paquetes en dicha topología.

DIAGRAMA DE TOPOLOGIA:

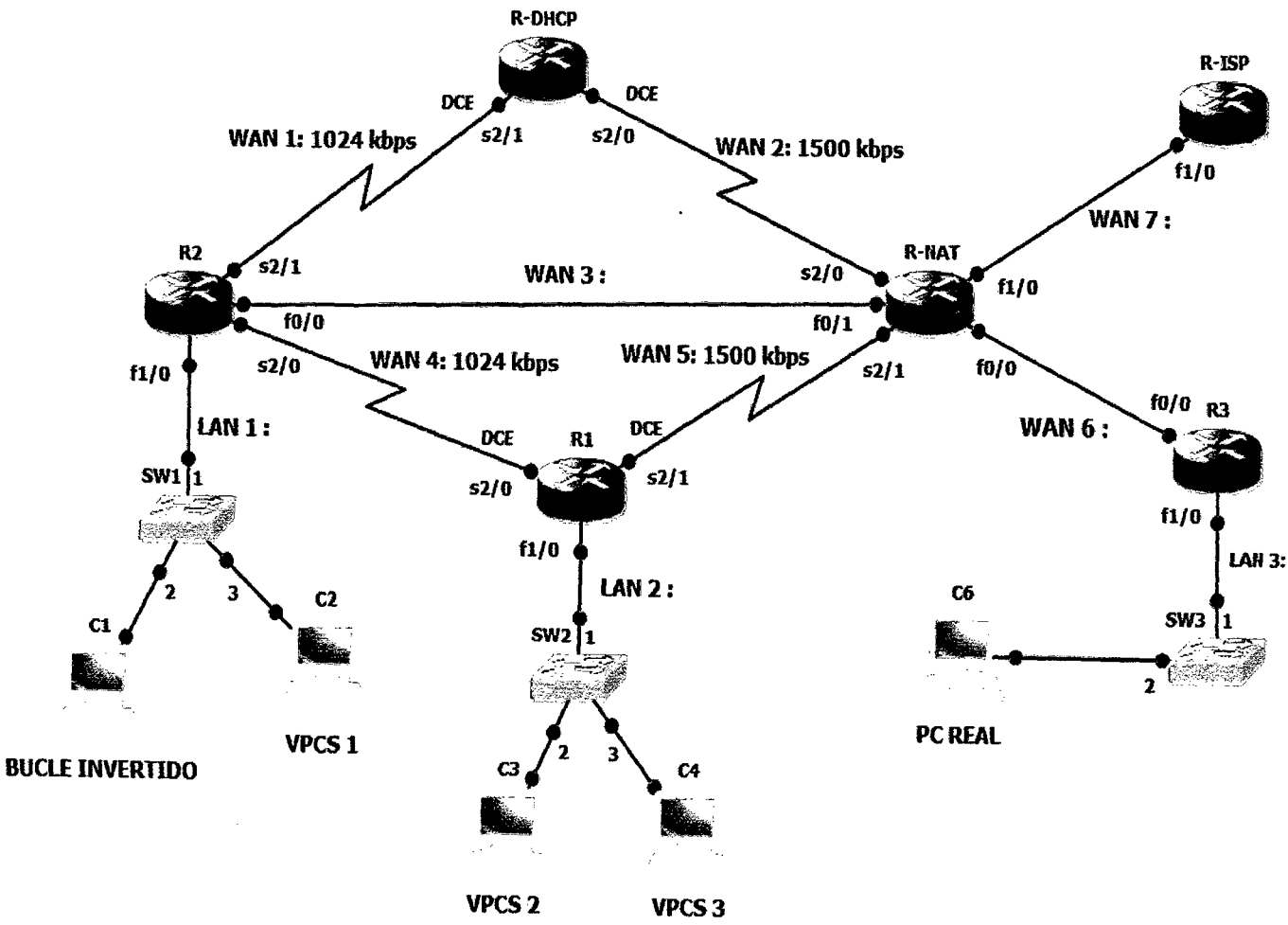


Fig. 4.13.1 Diagrama de topología en GNS3.

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN:

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s2/0	172.16.4.13	255.255.255.30	No aplicable
	s2/1	172.16.4.18	255.255.255.30	No aplicable
	f1/0	172.16.2.1	255.255.255.0	No aplicable
R2	s2/0	172.16.4.14	255.255.255.30	No aplicable
	s2/1	172.16.4.1	255.255.255.30	No aplicable
	f0/0	172.16.4.9	255.255.255.30	No aplicable
	f1/0	172.16.1.1	255.255.255.0	No aplicable
R-NAT	s2/0	172.16.4.6	255.255.255.30	No aplicable
	s2/1	172.16.4.17	255.255.255.30	No aplicable
	f1/0	192.168.1.1	255.255.255.0	No aplicable
	f0/0	172.16.4.21	255.255.255.252	No aplicable
	f0/1	172.16.4.10	255.255.255.252	No aplicable
R-DHCP	s2/0	172.16.4.5	255.255.255.252	No aplicable
	s2/1	172.16.4.2	255.255.255.252	No aplicable
R-ISP	f1/0	192.168.1.2	255.255.255.0	No aplicable
R3	f0/0	172.16.4.22	255.255.255.252	No aplicable
	f1/0	172.16.3.1	255.255.255.0	No aplicable
C1	BUCLE INVERTIDO	DHCP	DHCP	DHCP
C4	VPCS	DHCP	DHCP	DHCP
C5	VPCS	DHCP	DHCP	DHCP
C2	VPCS	DHCP	DHCP	DHCP
PC REAL	NIC	DHCP	DHCP	DHCP

Tabla 4.13.1 Direccionamiento IP para las Redes

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

Montar y conectar la red igual a la del Diagrama de topología.

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

Configure los routers de acuerdo a las siguientes instrucciones desde el modo de configuración:

PASO 1: Configure el nombre de host del router.

PASO 2: Deshabilite la búsqueda DNS.

PASO 3: Configure una contraseña de Modo EXEC.

PASO 4: Configure un mensaje del día.

PASO 5: Configure una contraseña para las conexiones de la consola.

PASO 6: Configure una contraseña para las conexiones de vty.

PASO 7: Configure el registro de datos sincrónico.

PASO 8: Guardar la configuración en cada router.

TAREA 3: CONFIGURAR Y ACTIVAR LAS DIRECCIONES SERIAL Y FASTETHERNET

Aplique Los siguientes comandos:

PASO1: Configuración para una interface serial DCE:

R1:

R1(config)# **interface serial 2/0**

R1(config-if)# **description conexion a R2**

R1(config-if)# **ip address 172.16.4.13 255.255.255.30**

R1(config-if)#**clock rate 64000**

R1(config-if)#**bandwidth 1024**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R2:

R2(config)# **interface serial 2/0**

R2(config-if)# **description conexion a R1**

R2(config-if)# **ip address 172.16.4.14 255.255.255.30**

R2(config-if)#**bandwidth 1024**

R2(config-if)# **no shutdown**

R2(config-if)# **exit**

PASO 2: Configuración para una interface fasEthernet:

R1:

R1(config)# **interface fasEthernet 1/0**

R1(config-if)# **description conexion a LAN 2**

R1(config-if)# **ip address 172.16.2.1 255.255.255.0**

R1(config-if)# **no shutdown**

R1(config-if)# **end**

R2:

R2(config)# **interface fasEthernet 0/0**

R2(config-if)# **description conexion a R-NAT**

R2(config-if)# **ip address 172.16.4.9 255.255.255.30**

R2(config-if)# **no shutdown**

R2(config-if)# **end**

R2(config)# **interface fasEthernet 1/0**

R2(config-if)# **description conexion a LAN 1**

R2(config-if)# **ip address 172.16.1.1 255.255.255.0**

R2(config-if)# **no shutdown**

R2(config-if)# **end**

PASO 2: Configurar las interfaces Loopback

En el router ISP configure las 3 interfaces loopback:

Loopback 1: 200.200.200.100 /32

Loopback 2: 200.200.200.200 /32

Loopback 3: 200.200.200.400 /32

ISP:

ISP(config)#**interface loopback 1**

ISP(config)# **ip address 200.200.200.100 255.255.255.255**

ISP(config)# **exit**

NOTA: Seguir los mismos pasos para las demás routers.

TAREA 4: CONFIGURAR EL PROTOCOLO DE ENRUTAMIENTO OSPF.

PASO 1: Configure una ruta estática por defecto en el router R2 para alcanzar las direcciones loopback del router ISP.

R-NAT(config)#**ip route 0.0.0.0 0.0.0.0 192.168.1.2**

PASO 2: Configure el protocolo de enrutamiento OSPF en todos los routers de la red para la conectividad.

R-NAT#**configure terminal**

R-NAT(config)#**router ospf 100**
R-NAT(config-router)#**network 172.16.1.0 0.0.0.255 area 0**
R-NAT(config-router)#**network 172.16.4.0 0.0.0.30 area 0**
R-NAT(config-router)#**network 172.16.4.8 0.0.0.30 area 0**
R-NAT(config-router)#**network 172.16.4.12 0.0.0.30 area 0**
R-NAT(config-router)#**default-information originate**
R-NAT(config-router)#**exit**
R2(config)#**router ospf 100**
R2(config-router)#**network 172.16.1.0 0.0.0.255 area 0**
R2(config-router)#**network 172.16.4.12 0.0.0.30 area 0**
R2(config-router)#**network 172.16.4.16 0.0.0.30 area 0**
R2(config-router)#**passive-interface fastethernet 1/0**
R2(config-router)#**end**

R3(config)#**router ospf 100**
R3(config-router)# **network 172.16.3.0 0.0.0.255 area 0**
R3(config-router)# **network 172.16.4.20 0.0.0.30 area 0**
R3(config-router)# **passive-interface fastethernet 1/0**
R3(config-router)#**end**

NOTA: Seguir los mismos pasos para la configuración de los demás routers.

TAREA 5: CONFIGURE DHCP EN EL ROUTER R-DHCP

PASO 1: Configure las tres redes LAN en el router R-DHCP.

R-DHCP:

R-DHCP(config)#**ip dhcp pool LAN_1**
R-DHCP (dhcp-config)#**network 172.16.1.0 255.255.255.0**
R-DHCP (dhcp-config)#**default-router 172.16.1.1**
R-DHCP (dhcp-config)#**dns-server 200.48.225.130**
R-DHCP (dhcp- config)#**exit**
R-DHCP (config)#**ip dhcp excluded-address 172.16.1.1 172.16.1.10**
R-DHCP (config)#**ip dhcp pool LAN_2**
R-DHCP (dhcp-config)#**network 172.16.2.0 255.255.255.0**
R-DHCP R1(dhcp-config)#**default-router 172.16.2.1**
R-DHCP (dhcp-config)#**dns-server 200.48.225.130**
R-DHCP (dhcp-config)#**exit**
R-DHCP (config)# **ip dhcp excluded-address 172.16.2.1 172.16.2.10**
R-DHCP (config)#**ip dhcp pool LAN_3**
R-DHCP (dhcp-config)#**network 172.16.3.0 255.255.255.0**
R-DHCP (dhcp-config)#**default-router 172.16.3.1**
R-DHCP (dhcp-config)#**dns-server 200.48.225.130**
R-DHCP (dhcp-config)#**exit**
R-DHCP (config)# **ip dhcp excluded-address 172.16.3.1 172.16.3.10**

PASO 2: Debido a que el servidor de DHCP y los clientes DHCP no se encuentran en la misma subred, configure R-DHCP para que envíe broadcasts de DHCP a R1, R2 y R3, que es el servidor de DHCP, mediante el comando de configuración de interfaz **ip helper-address** este comando debe configurarse en cada una de las interfaces.

R1(config)#**interface fa1/0**

R1(config-if)#**ip helper-address 172.16.4.2**

R2(config)#**interface fa1/0**

R2(config-if)#**ip helper-address 172.16.4.2**

R3(config)#**interface fa1/0**

R3(config-if)#**ip helper-address 172.16.4.5**

TAREA 6: CONFIGURACION DE NAT

PASO 1: Configurar NAT estática:

R-NAT:

R-NAT(config)#**ip nat inside source static 172.16.1.2 200.200.1.2**

R-NAT(config)#**ip nat inside source static 172.16.1.3 200.200.1.3**

R-NAT(config)#**ip nat inside source static 172.16.2.2 200.200.2.2**

R-NAT(config)#**ip nat inside source static 172.16.2.3 200.200.2.3**

R-NAT(config)#**ip nat inside source static 172.16.3.2 200.200.3.2**

R-NAT (config)#**interface fastEthernet 1/0**

R-NAT (config-if)#**ip nat outside**

R-NAT (config-if)#**exit**

R-NAT (config)#**interface fastEthernet 0/0**

R-NAT (config-if)#**ip nat inside**

R-NAT (config-if)#**exit**

R-NAT (config)#**interface serial 2/0**

R-NAT (config-if)#**ip nat inside**

R-NAT (config-if)#**exit**

R-NAT (config)#**interface serial 2/1**

R-NAT (config-if)#**ip nat inside**

R-NAT (config-if)#**exit**

PASO 2: Configuración de NAT dinámica:

R-NAT:

R-NAT(config)#**ip nat pool unprg 200.200.200.4 200.200.200.14 netmask 255.255.255.192**

R-NAT (config)#**ip access-list extended 1**

R-NAT (config-ext-nacl)# **permit ip 172.16.1.0 0.0.0.255 any**

R-NAT (config-ext-nacl)# **permit ip 172.16.2.0 0.0.0.255 any**

R-NAT (config-ext-nacl)# **permit ip 172.16.3.0 0.0.0.255 any**

R-NAT (config)#**ip nat inside source list 1 pool unprg**

R-NAT (config)#**exit**

NOTA: También se especifican las interfaces NAT internas y externas cuando se quiere configurar solo NAT dinámica, pero en este caso ya fueron especificadas en el apartado anterior.

PASO 3: Configuración de PAT o NAT con sobrecarga:

R-NAT:

R-NAT (config)#**ip access-list extended 2**

R-NAT (config-ext-nacl)# **permit ip 172.16.1.0 0.0.0.255 any**

R-NAT (config-ext-nacl)# **permit ip 172.16.2.0 0.0.0.255 any**

R-NAT (config-ext-nacl)# **permit ip 172.16.3.0 0.0.0.255 any**

R-NAT (config)#**ip nat inside source list 2 interface fastethernet 1/0 overload**

R1(config)#**exit**

NOTA: También se especifican las interfaces NAT internas y externas cuando se quiere configurar solo PAT, pero en este caso ya fueron especificadas en el apartado de NAT estática. Para denegar alguna host utilice el comando **deny ip 172.16.1.2 0.0.0.0** dentro de la Access-list.

TAREA 7: CONFIGURAR LOS EQUIPOS DE HOST.

Configurar las direcciones IP y gateways por defecto como se indican en la tabla de direccionamiento de las interfaces Ethernet de C1, C2, C3 y C4 (VPCS) y PC REAL.

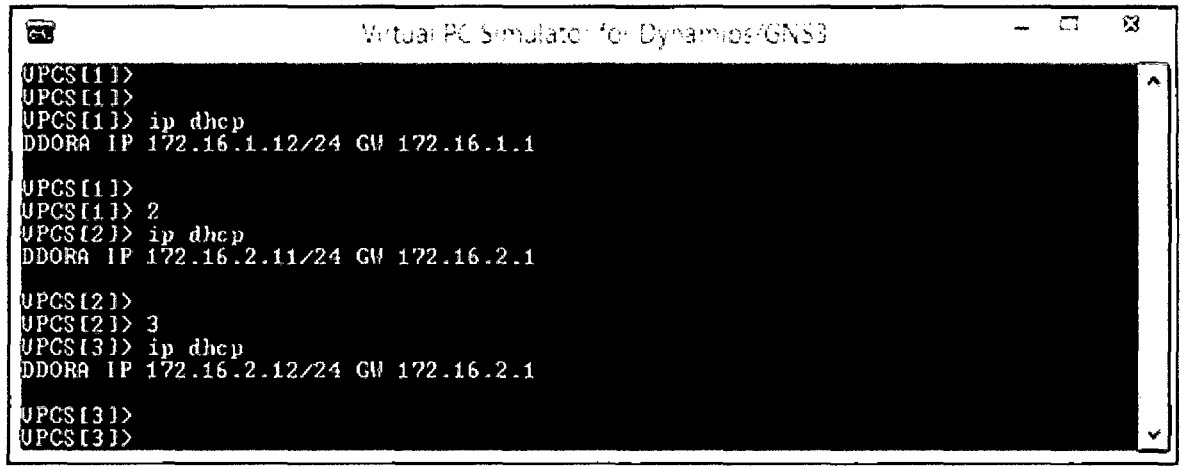


Fig. 4.13.2 Configuración de las direcciones IP en el VPCS.

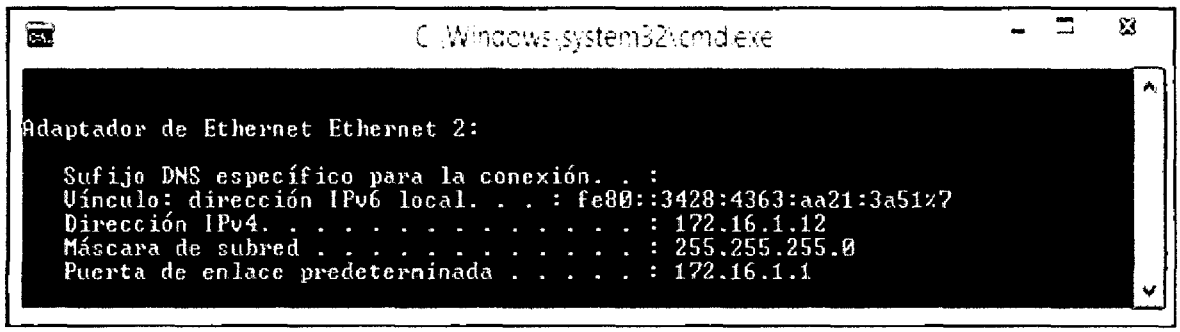


Fig. 4.13.3 Verificación de la interface del bucle invertido.

TAREA 8: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

PASO 1: Verificar el direccionamiento IP y las interfaces.

R1#**show ip interface brief**

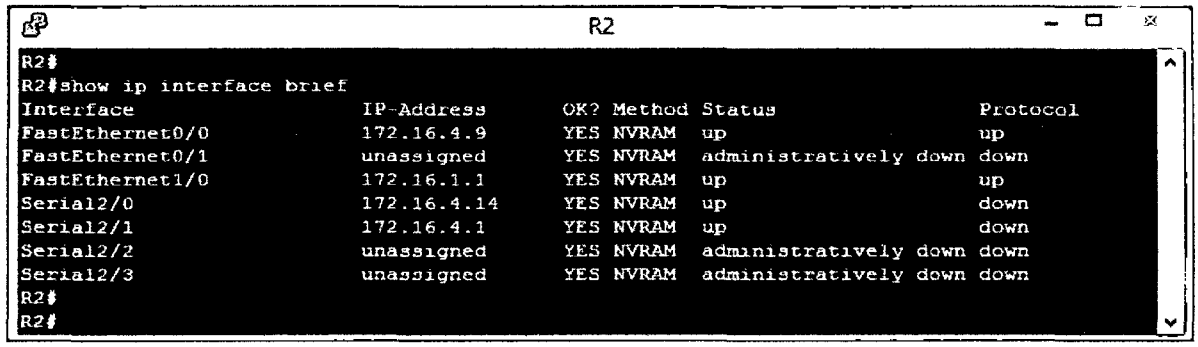


Fig. 4.13.4 Tabla ip de interface brief de R2.

NOTA: Verificar que las interfaces de los demás routers tengan la adecuada dirección IP y estén activas.

PASO 2: Verificar la configuración de los router. Use los comandos **show ip route** para verificar el contenido de la tabla de enrutamiento.

R2#**show ip route**

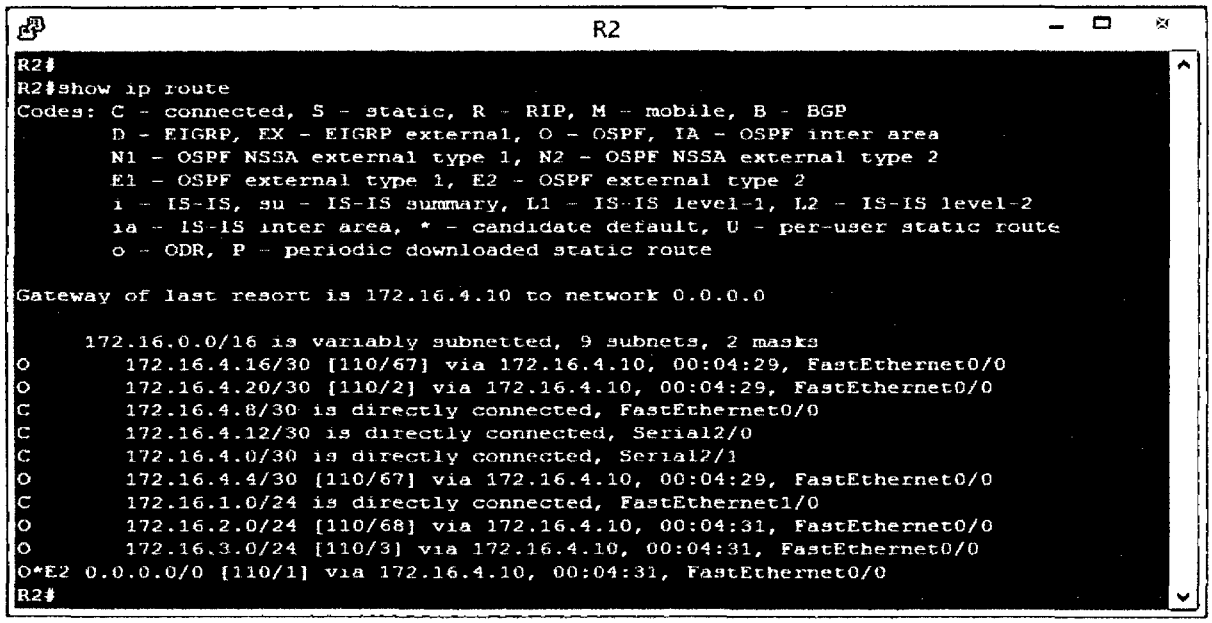


Fig. 4.13.5 Tabla de enrutamiento de R2.

NOTA: Verificar de igual manera la tabla de enrutamiento de los demás routers.

PASO 3: Verificar el correcto funcionamiento de DHCP en el router R-DHCP, para ello usamos el siguiente comando.

R-DHCP#**show ip dhcp binding**

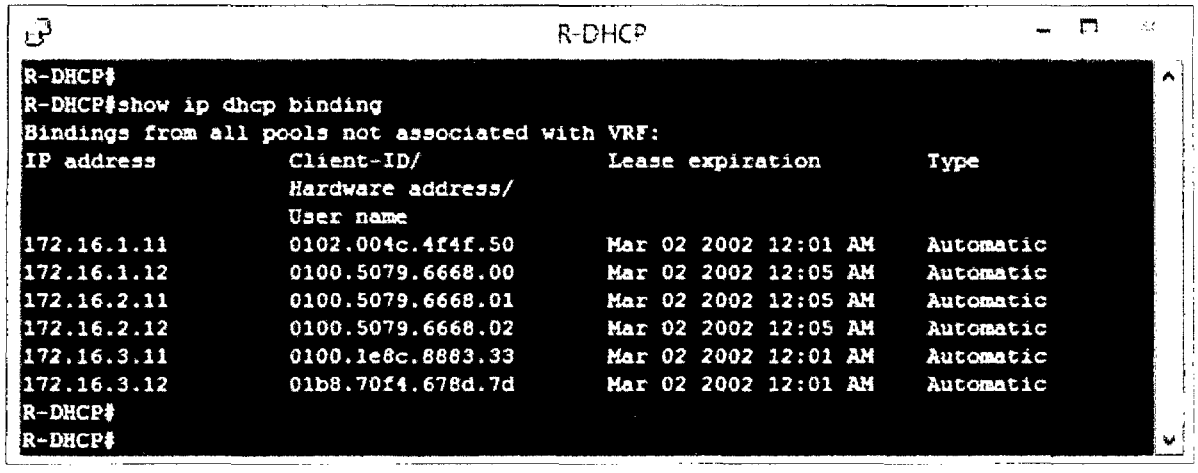


Fig. 4.13.6 Verificando de DHCP en el router R-DHCP.

PASO 4: Verificar la configuración de NAT estático, dinámico y PAT.

Para la verificación de NAT pacer ping desde la C1 hasta una de las interfaces loopback del ISP, seguidamente utilice los siguientes comandos mencionados en el router R-NAT

R-NAT#show ip nat translations

R-NAT#show ip nat statistics

PASO 5: Verificar que hay conectividad completa en la red.

Use el comando **ping** para verificar la conectividad.

R2#**ping 172.16.2.1**

R2#**ping 172.16.3.1**

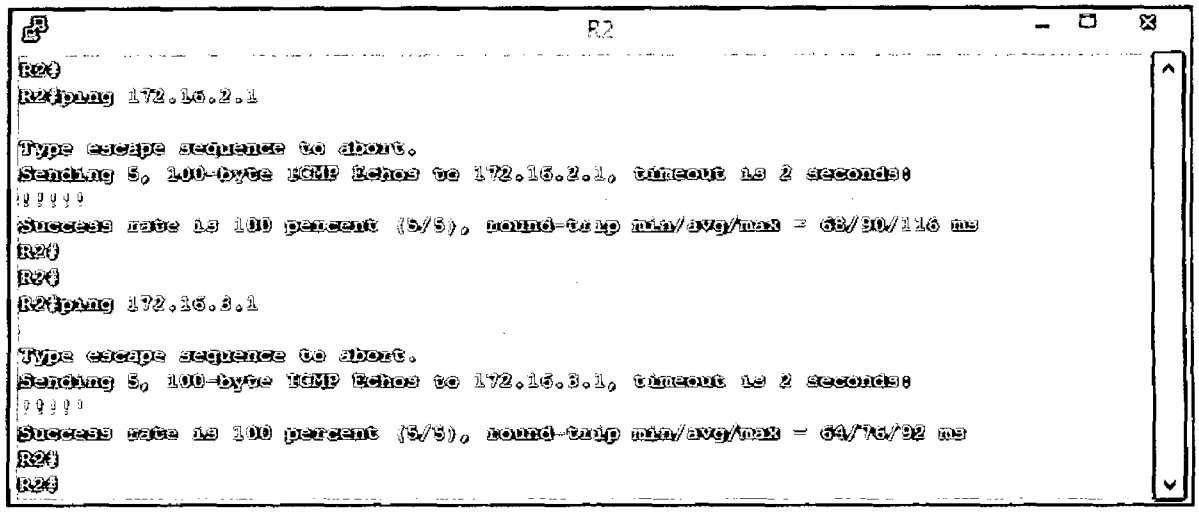


Fig. 4.13.7 Prueba de conectividad entre routers.

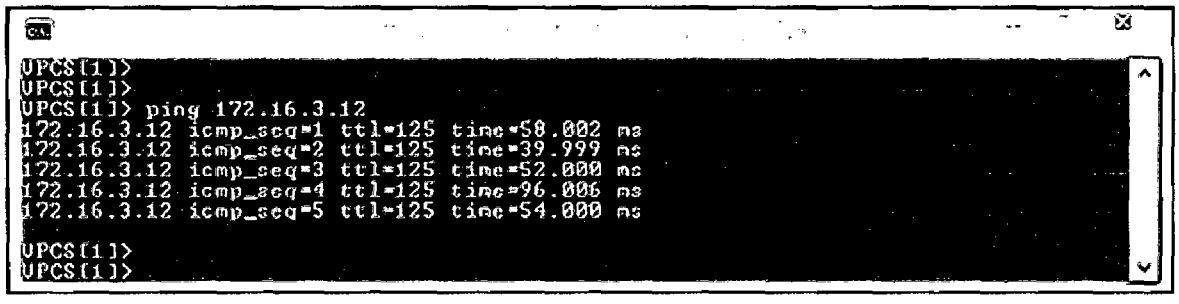


Fig. 4.13.8 Prueba de conectividad entre host desde C2 a PC real.

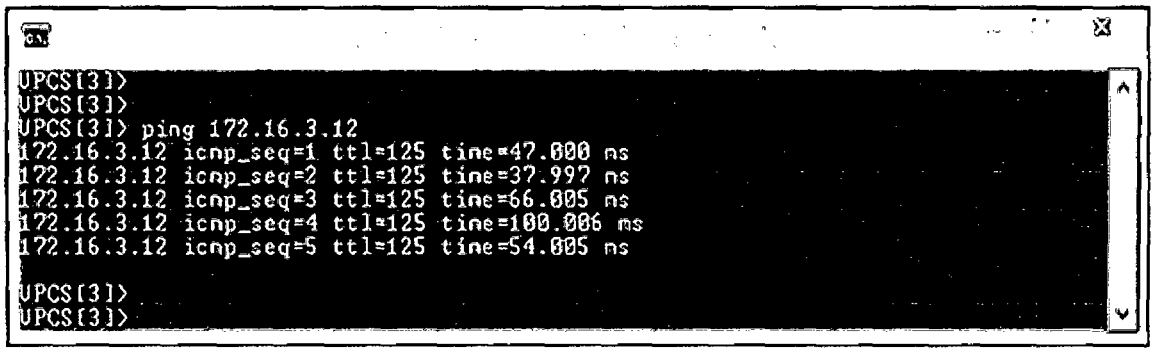


Fig. 4.13.9 Prueba de conectividad entre host desde C4 a PC real.

TAREA 9: ANALISIS DEL TRAFICO DE PAQUETES

PASO 1: Medición de la Latencia

Para la medición de la latencia se realizó 10 muestras sucesivas de 100 ping desde el C1 (Bucle invertido) hacia la PC REAL considerando un tamaño de trama de 64, 512 y 1518 bytes como se especifica en el RFC 2544.

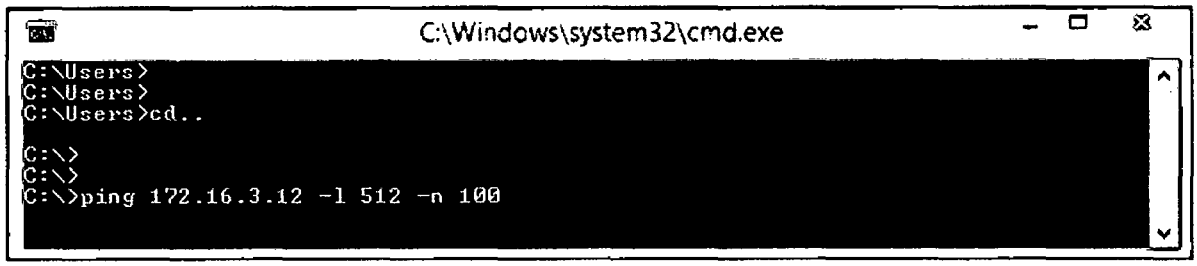


Fig. 4.13.10 Forma de medición de la latencia.

En la Figura 4.13.9 se puede observar el envío de 100 ping con una trama de 1518 hacia la dirección 172.16.3.12

En las Tablas posteriores se detallan los valores de la Latencia que se ha obtenido una vez realizadas todas las muestras.

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	**40**	**35**	**45**	**34**	**38**	**50**	**37**	**40**	**37**	**33**	**38.9**
Tiempo Máximo (ms)	**181**	**305**	**247**	**295**	**383**	**286**	**356**	**366**	**368**	**228**	**301.5**
Tiempo Promedio (ms)	**79**	**156**	**101**	**131**	**124**	**127**	**132**	**101**	**108**	**94**	**115.3**

Tabla 4.13.2 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	512										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	37	56	45	43	43	56	43	52	34	39	44.8
Tiempo Máximo (ms)	235	445	286	280	317	405	298	451	234	280	323.1
Tiempo Promedio (ms)	104	143	101	127	124	144	122	138	104	105	121.2

Tabla 4.13.3 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1518										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	44	48	54	45	45	45	48	54	47	41	47.1
Tiempo Máximo (ms)	431	402	439	225	230	248	492	452	382	217	351.8
Tiempo Promedio (ms)	167	123	136	115	116	123	123	130	109	111	125.3

Tabla 4.13.4 Comparación de datos obtenidos de las diferentes tramas.

LATENCIA			
Tamaño de Trama (bytes)	64	512	1518
Tiempo Mínimo (ms)	38.9	44.8	47.1
Tiempo Máximo (ms)	301.5	323.1	351.8
Tiempo Promedio (ms)	115.3	121.2	125.3

Tabla 4.13.5 Comparación de datos obtenidos de las diferentes tramas.

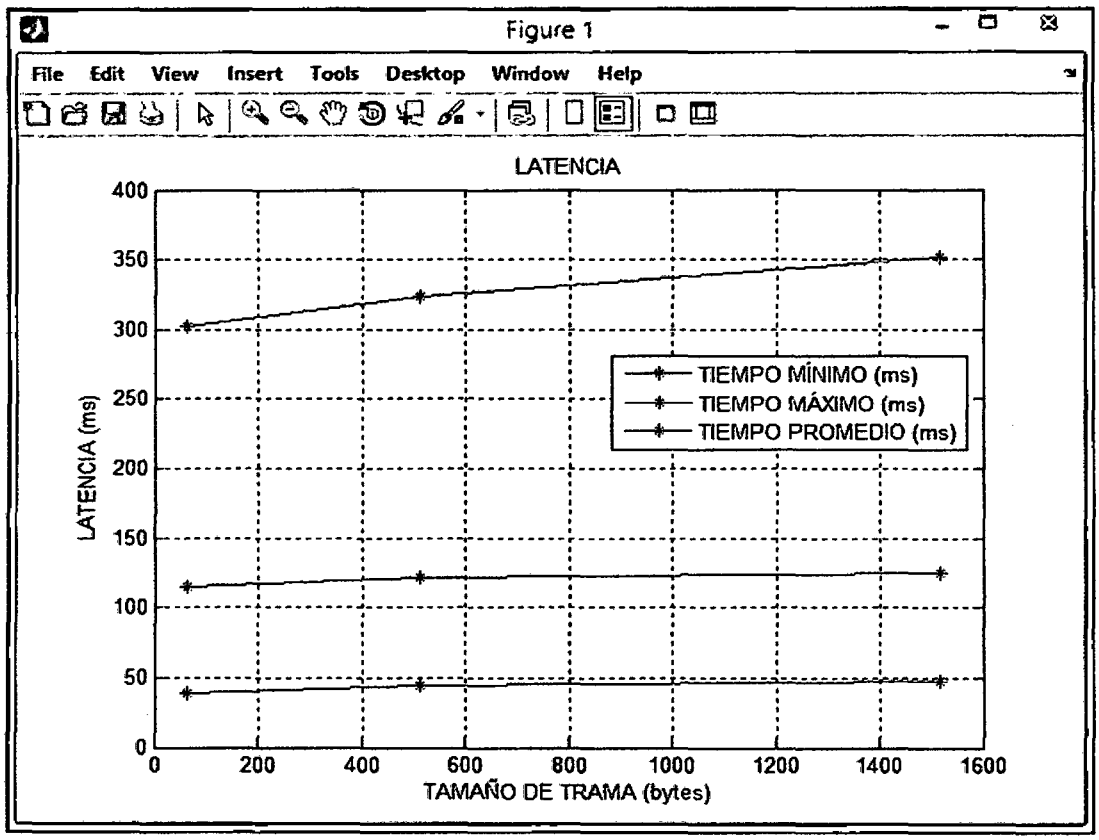


Fig. 4.13.11 Datos representados gráficamente de la variación de la latencia.

De acuerdo con los datos obtenidos, se puede observar claramente que los valores mínimo (color azul), máximo (color rojo) y promedio (color verde) de la latencia de la red se incrementan conforme se envía una trama de longitud mayor, en este caso con la trama de 1518 bytes se obtiene una latencia promedio de 125.3 ms a diferencia de una trama de 64 bytes con 115.3 ms.

PASO 2: Medición del Throughput

Para la medición del Throughput y Jitter se envió una cantidad de tramas a velocidades diferentes durante 20 segundos, hasta encontrar la máxima cantidad de tramas recibidas sin que se produzcan perdidas de las mismas en el router y PC REAL. Como se utilizó Jperf el cliente será el encargado de enviar los paquetes y el servidor los recibirá, indicando la cantidad de paquetes que llegaron correctamente considerando un tamaño del paquete UDP de 750, 1125, 1500 y 1470 (default) bytes, tal como se especifica en el RFC 768.

Configuración del Jperf como servidor para medir Throughput:

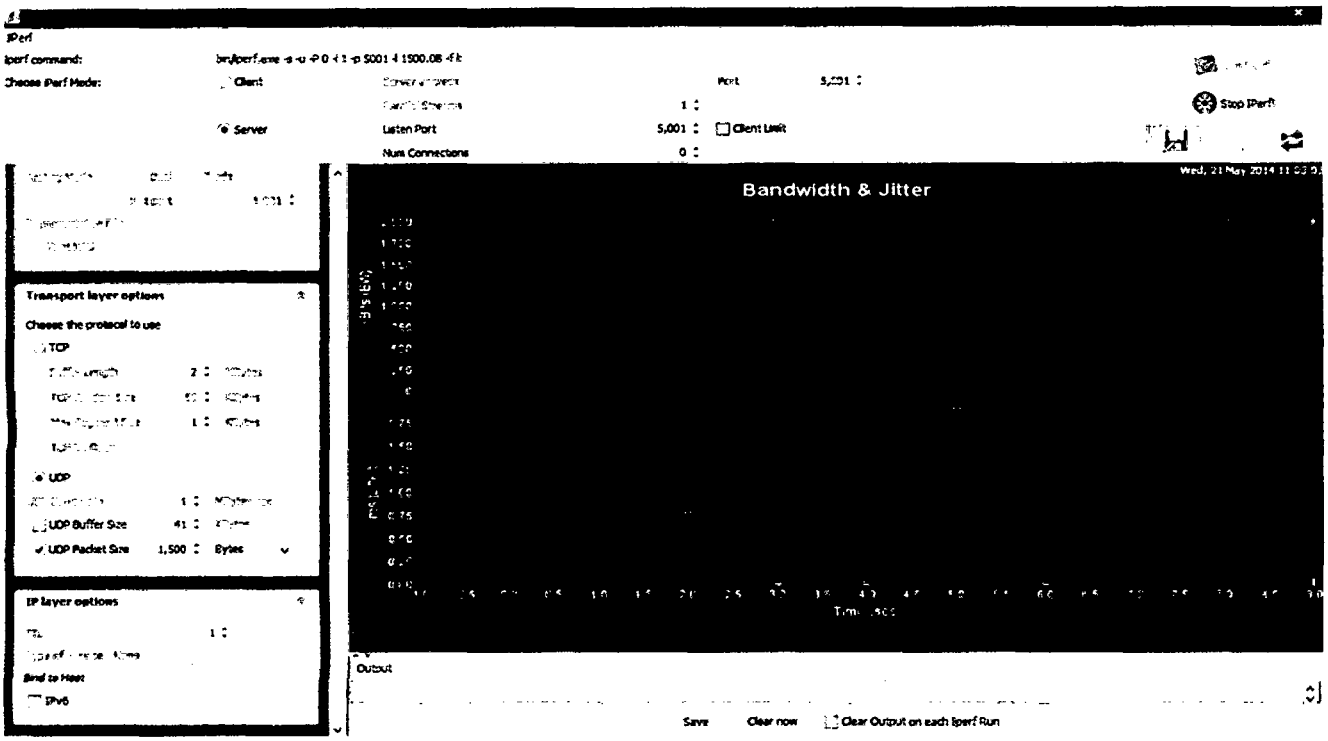


Fig. 4.13.12 Gráfica de Bandwidth y Jitter.

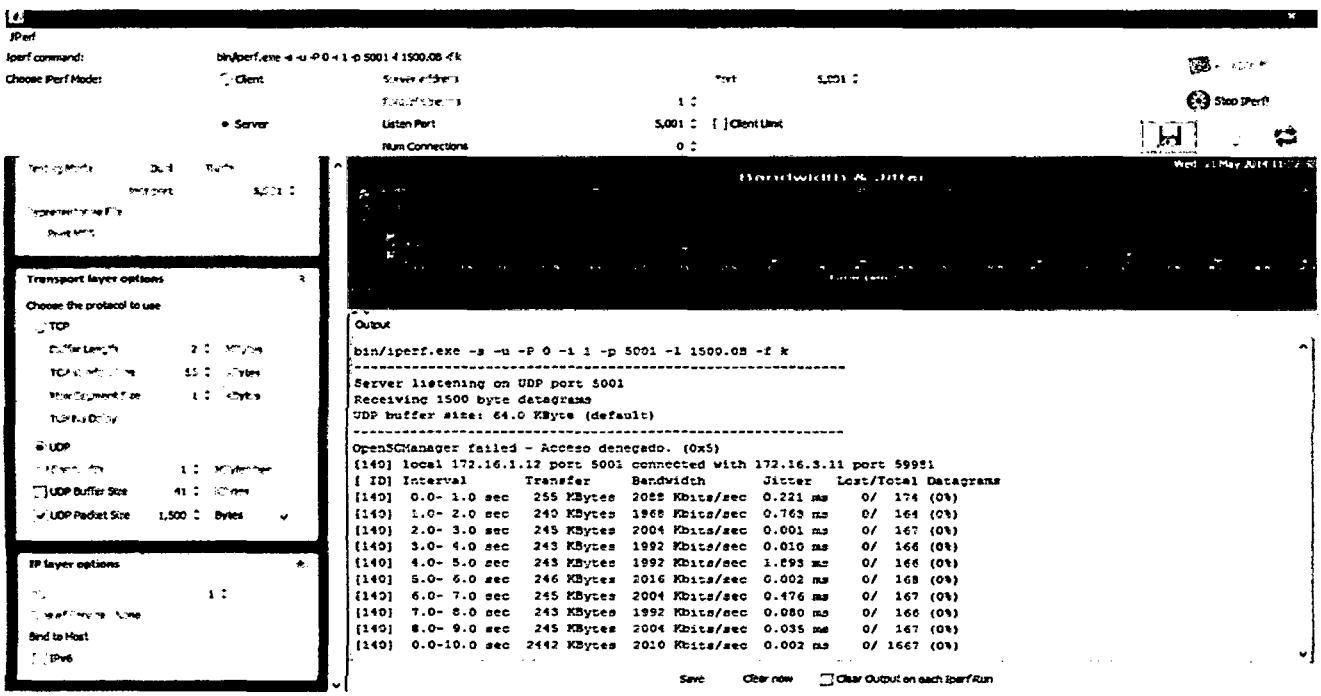


Fig. 4.11.13 Resultados al medir Throughput como servidor.

Configuración del Jperf como cliente para medir Throughput:

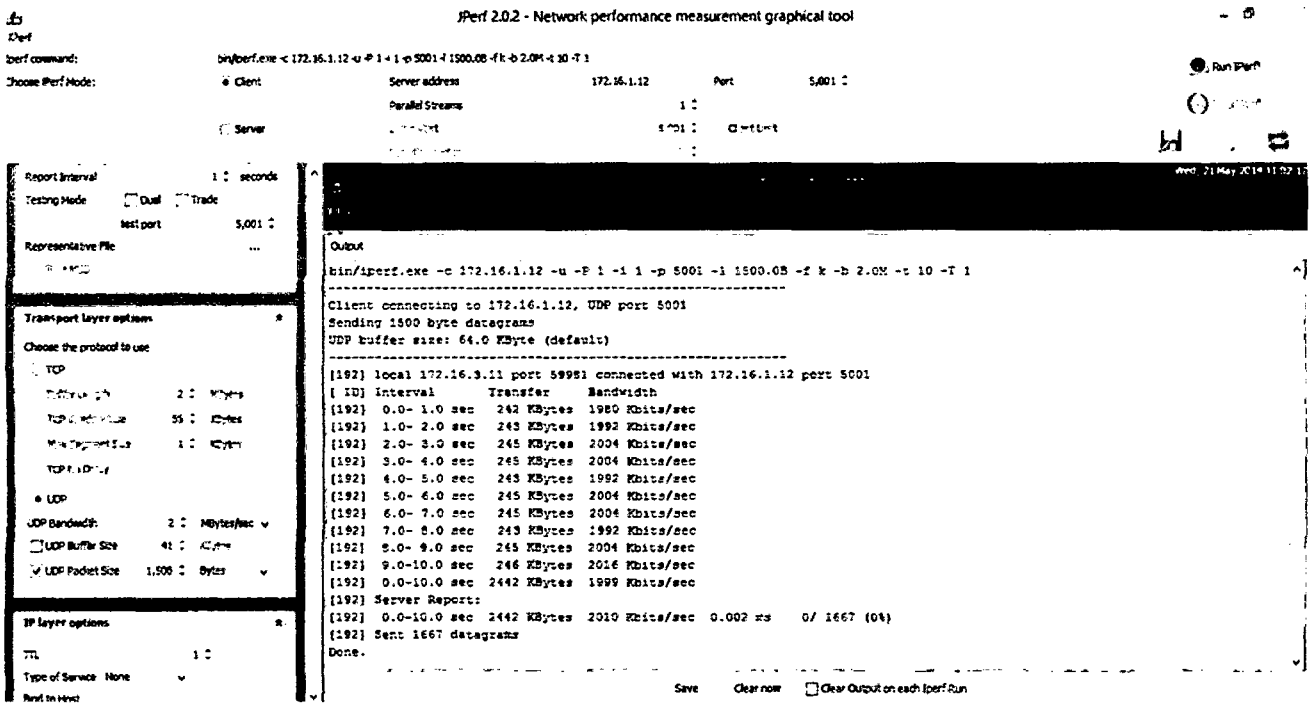


Fig. 4.13.14 Resultados del Jperf como Cliente al medir Throughput.

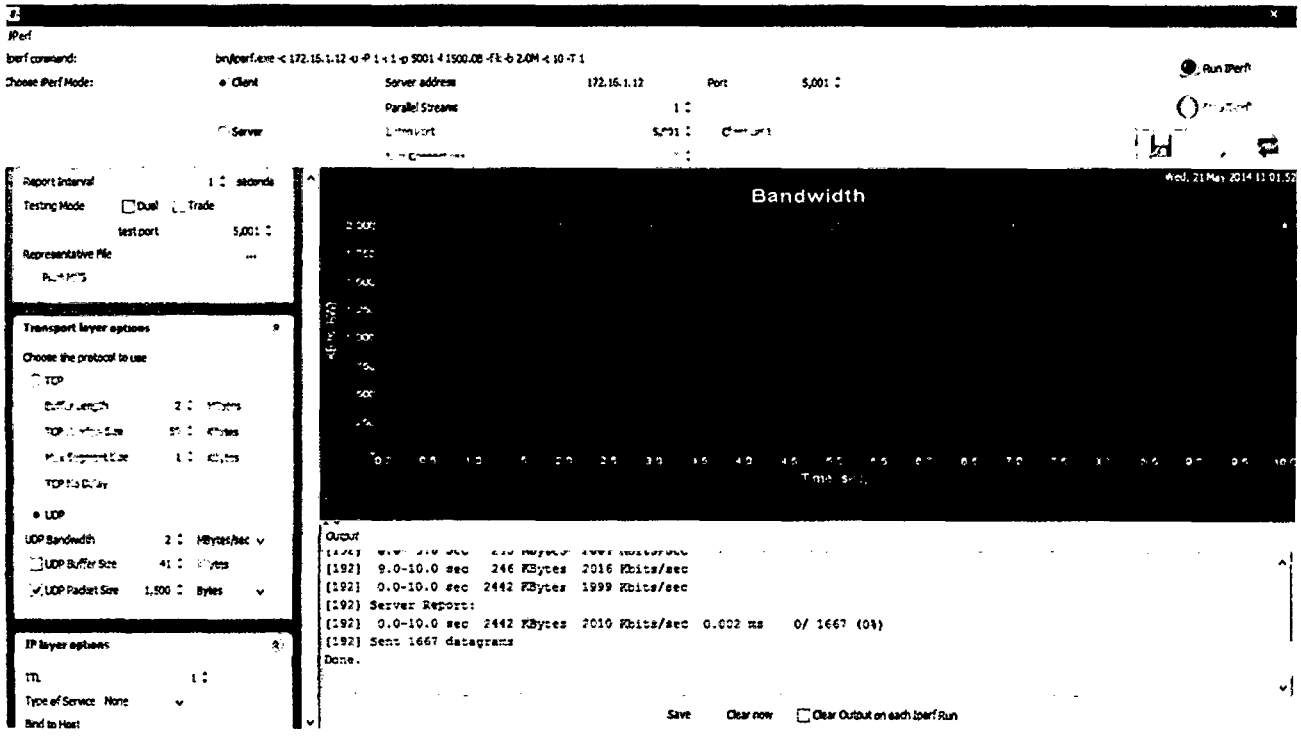


Fig. 4.11.15 Gráfica de Bandwidth.

En las siguientes Tablas se detalla los valores del Throughput obtenidos una vez realizada todas las muestras.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**2**	**2**	**2**
Velocidad de Rx (Mbps)	**1.99**	**2**	**2**
Tramas Transmitidas	**3330**	**2220**	**1667**
Tramas Recibidas	**3330**	**2220**	**1667**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**333**	**222**	**166**

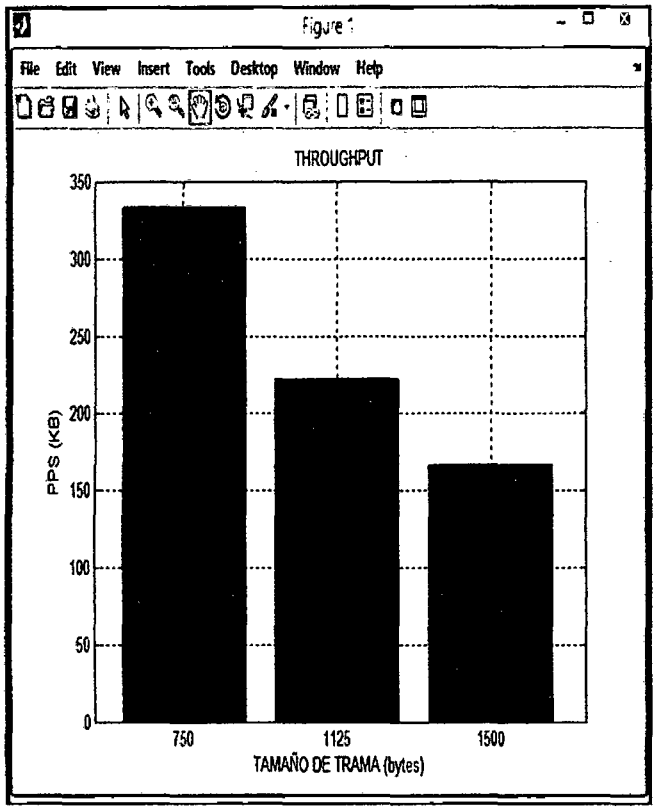
Tabla 4.13.6 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**1**	**2**	**6**
Velocidad de Rx (Mbps)	**0.99**	**1.99**	**6**
Tramas Transmitidas	**851**	**1700**	**5096**
Tramas Recibidas	**851**	**1700**	**5096**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**85**	**170**	**510**

Tabla 4.13.7 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**9**	**10**	**11**
Velocidad de Rx (Mbps)	**9**	**10**	**10.56**
Tramas Transmitidas	**7648**	**8497**	**9348**
Tramas Recibidas	**7648**	**8497**	**9103**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**245 (2.6%)**
Tramas Recibidas (pps)	**766**	**850**	**932**

Tabla 4.13.8 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.



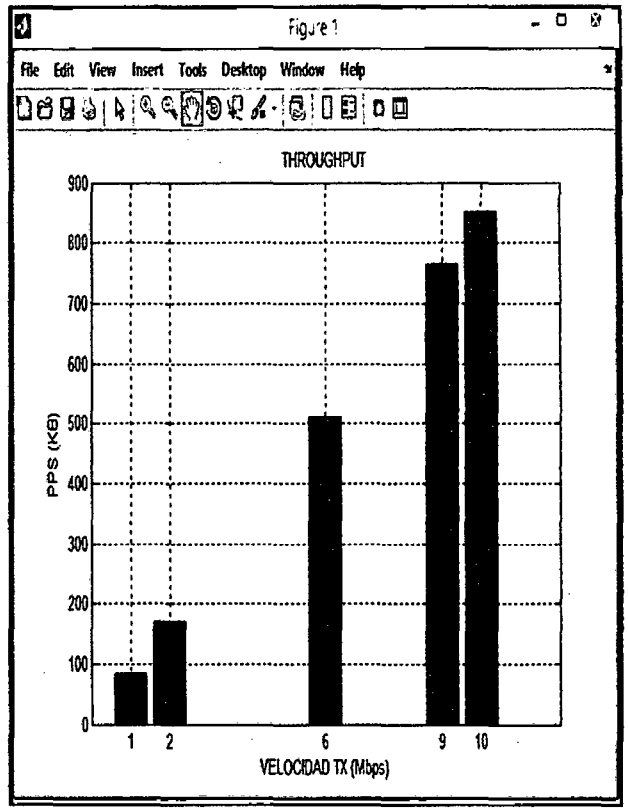


Fig. 4.13.16 PPS vs. Tamaño de Trama.

Fig. 4.13.17 PPS vs. Velocidad Tx.

En la figura 4.13.20, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 750 bytes, 1125 bytes y 1500 bytes los cuales han utilizado una velocidad de Tx constante de 2 Mbps, en la gráfica se puede observar claramente que al enviar una trama de 750 bytes se envía 333 pps, con una trama de 1125 se envía 222 pps y con una trama de 1500 se envía 166 pps.

Mientras en la figura 4.13.21, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 1470 bytes los cuales han utilizado una velocidad de Tx variada de: 1 Mbps, 2 Mbps, 6 Mbps, 9 Mbps y 10 Mbps, sin que se produzcan perdidas en el envío, como los datos que se muestran en la tabla 4.13.8.

PASO 3: Medición del Jitter

Para la medición se envió datos UDP de longitud variable a velocidades diferentes de Throughput obtenida anteriormente durante 20 segundos. Como se utilizó anteriormente Jperf el cliente será el encargado de enviar los datos y el servidor los recibirá, indicando los valores de Jitter obtenidos durante la transmisión de los datos.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**2**	**2**	**2**
Velocidad de Rx (Mbps)	**1.99**	**2**	**2**
Tramas Transmitidas	**3330**	**2220**	**1667**
Tramas Recibidas	**3330**	**2220**	**1667**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**1.851**	**0.379**	**0.002**

Tabla 4.13.9 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**1**	**2**	**6**
Velocidad de Rx (Mbps)	**0.99**	**1.99**	**6**
Tramas Transmitidas	**851**	**1700**	**5096**
Tramas Recibidas	**851**	**1700**	**5096**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**1.394**	**0.177**	**0.049**

Tabla 4.13.10 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**9**	**10**	**11**
Velocidad de Rx (Mbps)	**9**	**10**	**10.56**
Tramas Transmitidas	**7648**	**8497**	**9348**
Tramas Recibidas	**7648**	**8497**	**9105**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**243 (2.6%)**
Jitter (ms)	**0**	**0**	**2.53**

Tabla 4.13.11 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

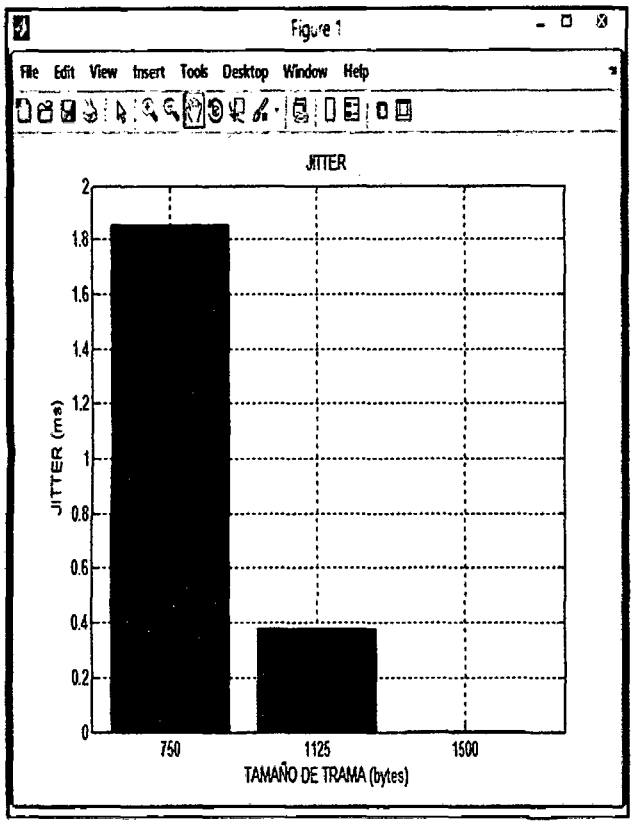


Fig. 4.13.18 Jitter vs. Tamaño de Trama

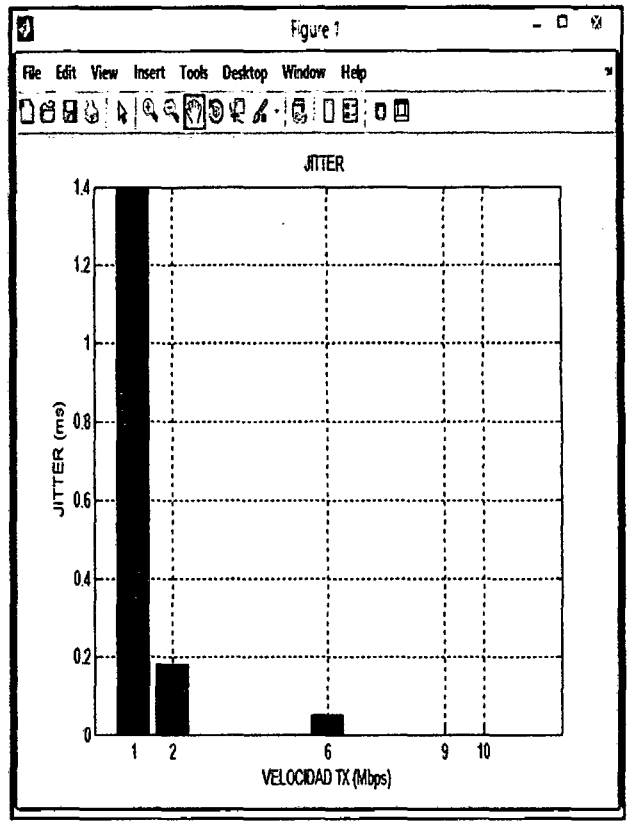


Fig. 4.13.19 Jitter vs. Velocidad Tx

En la figura 4.13.18 se observa los valores del Jitter obtenidos al enviar diferentes tamaños de paquete UDP como 750, 1125 y 1500 bytes utilizando una velocidad de Tx constante de 2 Mbps, se puede observar claramente que con una trama de 750 bytes se tiene un Jitter de 1.851 ms a diferencia de la trama de 1500 bytes en la cual se tiene un Jitter de 0.002 ms.

En la figura 4.11.23, se observa los valores del Jitter obtenidos al enviar paquetes UDP de 1470 bytes utilizando una velocidad de Tx que varía entre 1 Mbps, 2 Mbps, 6Mbps, 9 Mbps y 10 Mbps sin que se pierdan paquetes en la red, concluyendo también que a mayor ancho de banda mucho mayor será el jitter y pérdidas de datagramas.

Medición de Jitter a 9 Mbps:

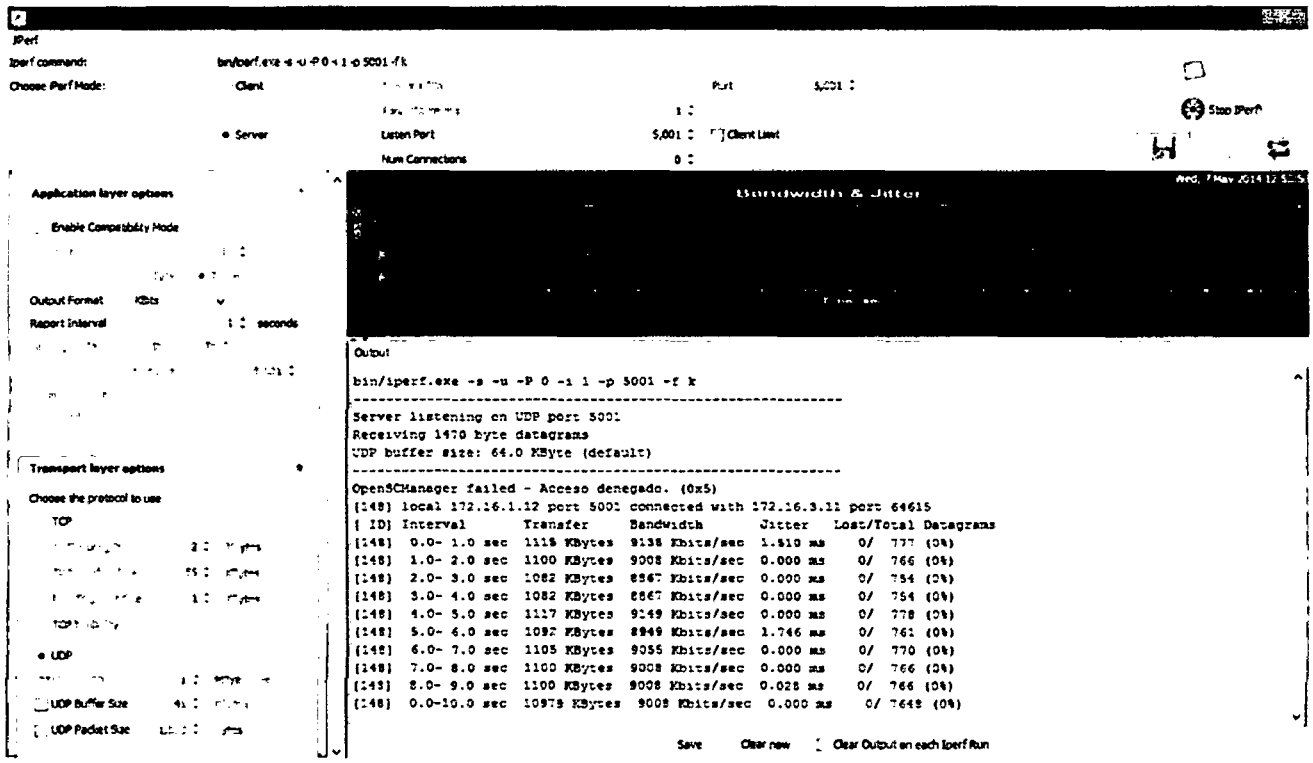


Fig. 4.13.20 Gráfica de Bandwidth y Jitter.

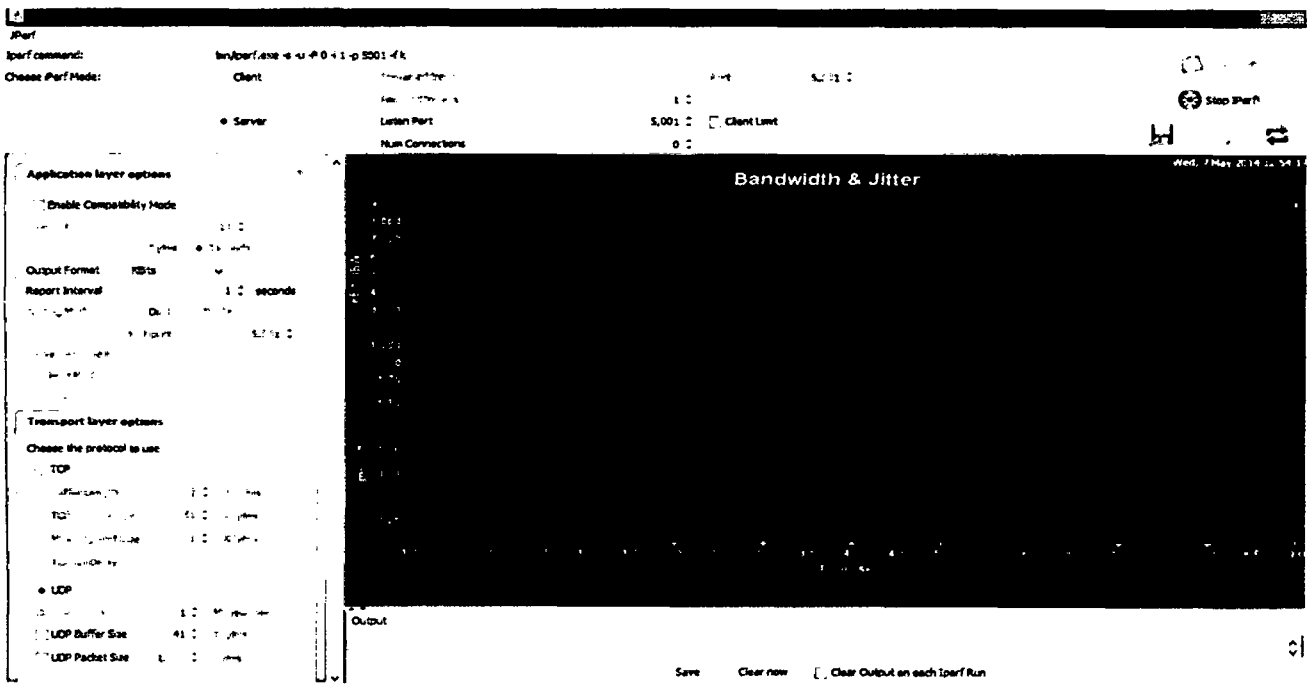


Fig. 4.13.21 Resultados al medir Throughput como servidor.

PASO 4: Captura de tráfico con Wireshark.

Capturar tráfico de paquetes en la interfaz s1/3 de R1.

- Captura de paquetes ICMP.

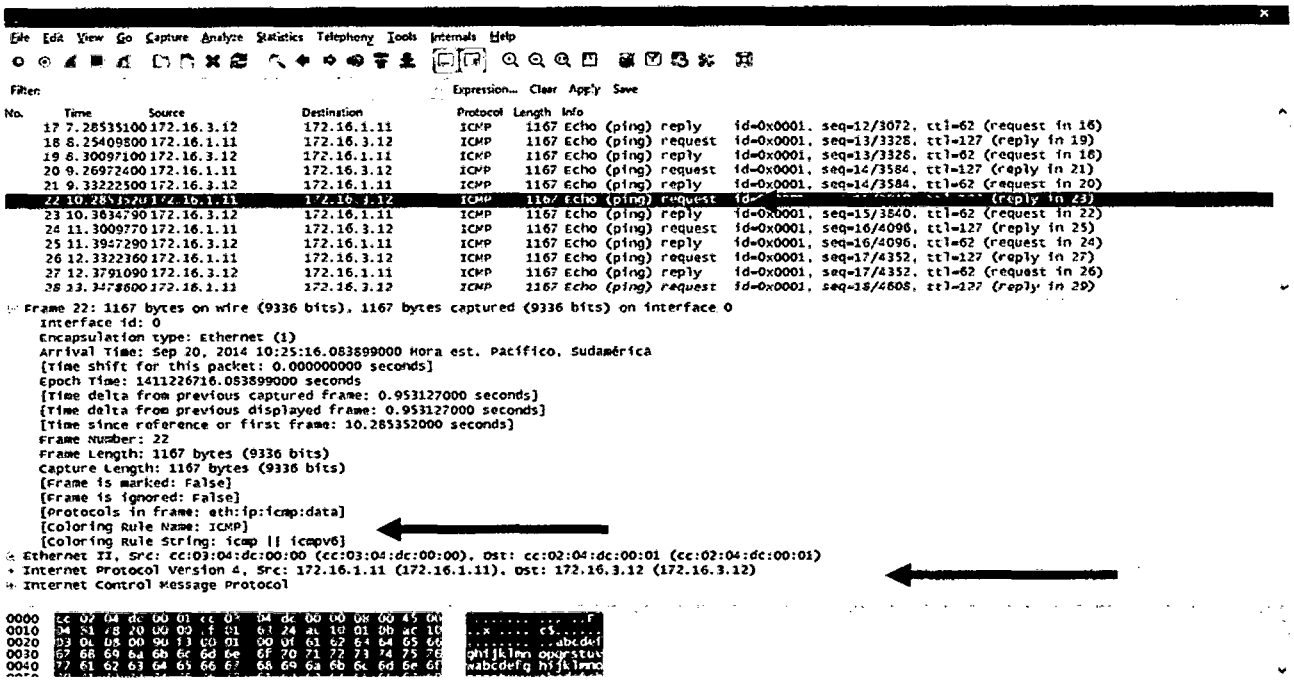


Fig. 4.13.22 Captura de paquetes ICMP con Wireshark.

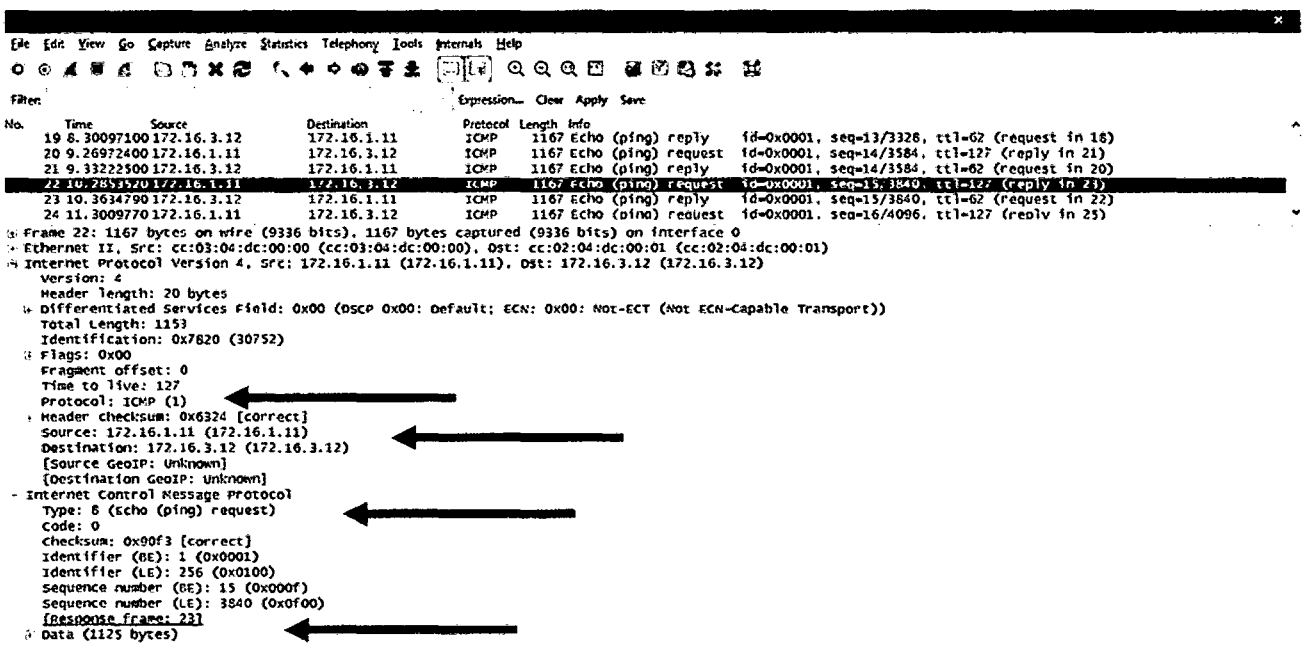


Fig. 4.13.23 Información detallada del origen y destino de paquetes.

- Protocolo de enrutamiento OSPF.

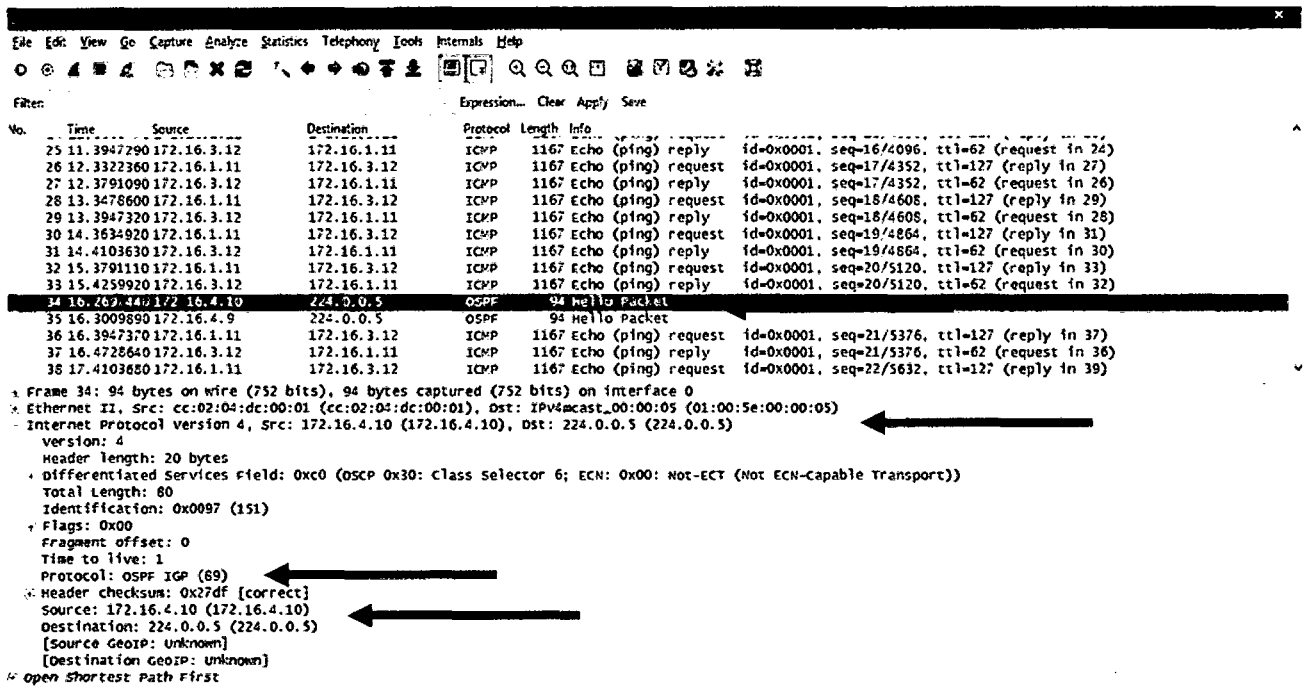


Fig. 4.13.24 Captura del protocolo de enrutamiento OSPF con wireshark.

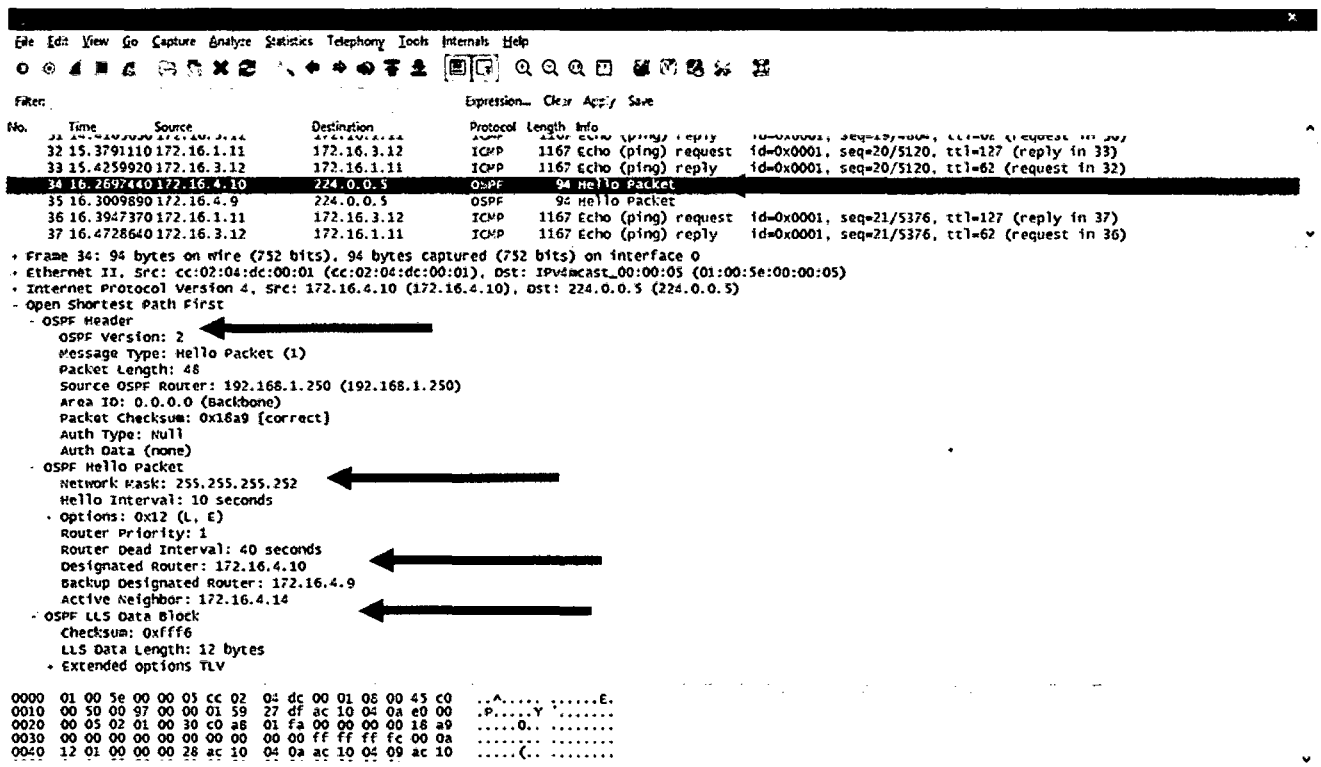


Fig. 4.13.25 Información detallada del protocolo OSPF.

LABORATORIO 4.14: CONFIGURACIÓN BÁSICA DE LISTAS DE CONTROL DE ACCESO

REVISIÓN TEÓRICA: Para la realización de esta práctica se deberá revisar conceptos de Listas de Control de Acceso.

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, el usuario podrá:

- Conectar una red según el diagrama de topología.
- Realizar tareas de configuración básica en los routers.
- Configurar y activar interfaces.
- Configurar el enrutamiento OSPF en todos los routers.
- Diseñar ACL nombradas estándar y nombradas ampliadas.
- Aplicar ACL nombradas estándar y nombradas ampliadas.
- Probar ACL nombradas estándar y nombradas ampliadas.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

ESCENARIO:

En esta práctica de laboratorio, se aprenderá a configurar la seguridad básica de red mediante listas de control de acceso. Se aplicarán ACL estándar y ampliadas. Utilice la dirección **192.168.10.0/24** para obtener el direccionamiento IP usando VLSM, teniendo los siguientes requisitos:

LAN 1 de R3: 170 direcciones IP de host.
LAN 2 de R1: 220 direcciones IP de host.
LAN 3 de R2: 200 direcciones IP de host.

Considerando también las redes que hay entre router y router (enlaces WAN).

Después de completar la configuración pruebe la conectividad entre los dispositivos de la red y finalmente analizará el tráfico de paquetes en dicha topología.

DIAGRAMA DE TOPOLOGÍA:

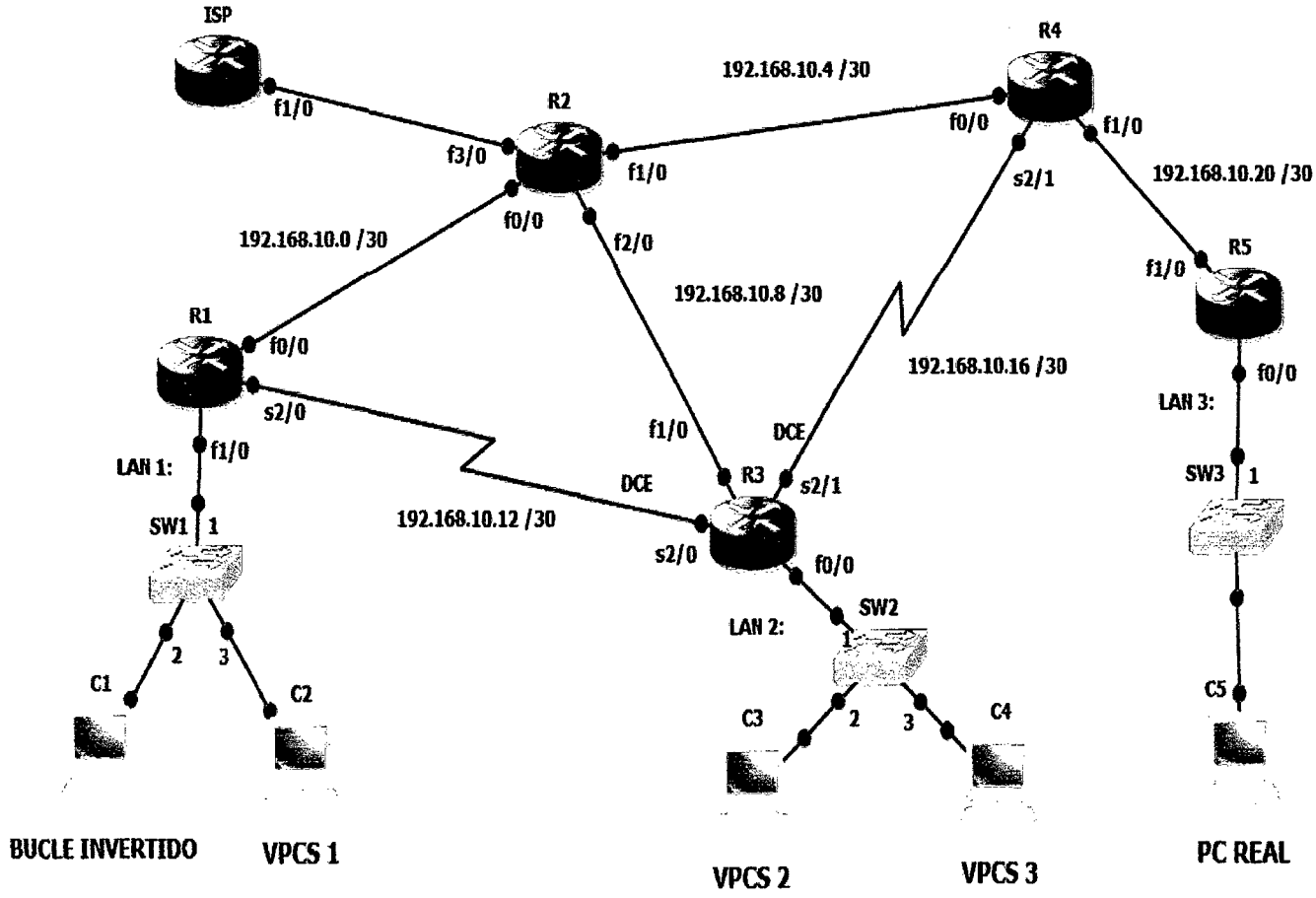


Fig. 4.14.1 Diagrama de topología en GNS3.

TABLA DE DIRECCIONAMIENTO:

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s2/0	192.168.10.13	255.255.255.252	No aplicable
	f0/0	192.168.10.1	255.255.255.252	No aplicable
	f1/0	192.168.1.1	255.255.255.0	No aplicable
R2	f3/0	200.200.200.1	255.255.255.252	No aplicable
	f0/0	192.168.10.2	255.255.255.252	No aplicable
	f1/0	192.168.10.5	255.255.255.252	No aplicable
	f2/0	192.168.10.9	255.255.255.252	No aplicable
R3	s2/0	192.168.10.14	255.255.255.252	No aplicable
	s2/1	192.168.10.18	255.255.255.252	No aplicable
	f0/0	192.168.2.1	255.255.255.252	No aplicable
	f1/0	192.168.10.10	255.255.255.252	No aplicable
R4	s0/0	192.168.10.17	255.255.255.252	No aplicable
	f0/0	192.168.10.6	255.255.255.252	No aplicable
	f1/0	192.168.10.21	255.255.255.252	No aplicable
R5	f0/0	192.168.3.1	255.255.255.0	No aplicable
	f1/0	192.168.10.22	255.255.255.252	No aplicable
ISP	f1/0	200.200.200.2	255.255.255.252	No aplicable
C1	BUCLE INVERTIDO	192.168.1.2	255.255.255.0	192.168.1.1
C2	VPCS	192.168.1.3	255.255.255.0	192.168.1.1
C3	VPCS	192.168.2.2	255.255.255.0	192.168.2.1
C4	VPCS	192.168.2.3	255.255.255.0	192.168.2.1
C5	NIC	192.168.3.2	255.255.255.0	192.168.3.1

Tabla 4.14.1 Direccionamiento IP para las Redes

TAREA 1: MONTAR LA RED EN GNS3

Montar y conectar la red igual a la del Diagrama de topología.

TAREA 2: REALIZAR LA CONFIGURACIÓN BÁSICA DEL ROUTER

Configure los routers R1, R2, R3, R4, y R5 de acuerdo a las siguientes instrucciones desde el modo de configuración:

Paso 1: Configure el nombre de host del router.

Paso 2: Deshabilite la búsqueda DNS.

Paso 3: Configure una contraseña de Modo EXEC.

Paso 4: Configure un mensaje del día.

Paso 5: Configure una contraseña para las conexiones de la consola.

Paso 6: Configure una contraseña para las conexiones de vty.

Paso 7: Configure el registro de datos sincrónico.

Paso 8: Guardar la configuración en cada router.

TAREA 3: CONFIGURAR Y ACTIVAR LAS DIRECCIONES SERIAL Y FASTETHERNET

PASO 1: Configurar las interfaces de los routers.

Configure las interfaces de los routers R1, R2, R3, R4, R5 e ISP con las direcciones IP de la tabla de direccionamiento que se encuentra al comienzo de esta práctica de laboratorio. Asegúrese de incluir la frecuencia de reloj en las interfaces DCE seriales de los routers R2 y R1, en R3 son interfaces DTE.

R2:

Configuración de las interfaces serial DCE:

R2(config)#**interface serial 1/0**

R2(config-if)#**ip address 200.200.200.1 255.255.255.252**

R2(config-if)#**description conexión a ISP**

R2(config-if)#**clock rate 64000**

R2(config-if)#**no shutdown**

R2(config-if)#**exit**

R2(config)#**interface serial 1/1**

R2(config-if)#**ip address 172.16.10.2 255.255.255.252**

R2(config-if)#**description conexión a R3**

R2(config-if)#**clock rate 64000**

R2(config-if)#**no shutdown**

R2(config-if)#**exit**

R2(config)#**interface serial 1/2**

R2(config-if)#**ip address 172.16.10.1 255.255.255.252**

R2(config-if)#**description conexión a R1**

R2(config-if)#**clock rate 64000**

R2(config-if)#**no shutdown**

R2(config-if)#**exit**

R3:

Configuración de la interface serial DTE:

R3(config)#**interface serial 1/2**

R3(config-if)#**ip address 172.16.10.2 255.255.255.252**

R3(config-if)#**description conexión a R2**

R3(config-if)#**no shutdown**

R3(config-if)#**exit**

Nota: Configurar las interfaces de los demás routers según corresponda.

PASO 2: Configurar las interfaces Loopback

En el router ISP configure las 3 interfaces loopback:

Loopback 1: 200.200.200.100 /32

Loopback 2: 200.200.200.200 /32

Loopback 3: 200.200.200.400 /32

ISP:

ISP(config)#**interface loopback 1**

ISP(config)# **ip address 200.200.200.100 255.255.255.255**

ISP(config)# **exit**

PASO 3: Guardar la configuración.

Guarde la configuración establecida de todos router con el comando **copy running-config startup-config**

TAREA 4: CONFIGURAR EL PROTOCOLO EIGRP

Configure el protocolo de enrutamiento EIGRP en todos los routers de la red para la conectividad.

R2(config)#**router eigrp 100**

R2(config-router)#**network 192.168.10.0 0.0.0.3**

R2(config-router)#**network 192.168.10.4 0.0.0.3**

R2(config-router)#**network 192.168.10.8 0.0.0.3**

R2(config-router)#**network 192.168.10.12 0.0.0.3**

R2(config-router)#**default-information originate**

R2(config-router)#**exit**

R5(config)#**router eigrp 100**

R5(config-router)#**network 192.168.10.16 0.0.0.3**

R5(config-router)# **network 192.168.3.0 0.0.0.255**

R5(config-router)#**passive-interface fastethernet 1/0**

R5(config-router)#**exit**

NOTA: Configurar el protocolo EIGRP de la misma manera en los demás routers.

TAREA 5: CONFIGURACIÓN DE LAS ACL

Paso 1: Configurar una ACL estándar en R1.

R1(config)#**access-list 1 deny 192.168.3.0 0.0.0.255**

R1(config)#**access-list 1 deny 192.168.2.0 0.0.0.255**

R1(config)#**access-list 1 permit 192.168.2.2 0.0.0.0**

R1(config)#**access-list 1 permit 192.168.3.2 0.0.0.0**

R1(config)#**interface serial 2/0**

R1(config-if)#**ip access-group 1 in**

R1(config-if)#**exit**

R1(config)#**interface fastethernet 0/0**

R1(config-if)#**ip access-group 1 in**

R1(config-if)#**exit**

Paso 2: Configurar una ACL estándar y nombrada en R5.

R5(config)#**ip access-list standard LISTA-1**

R5(config-std-nacl)#**deny 192.168.2.0 0.0.0.255**

R5(config-std-nacl)#**permit any**

R5(config)#**interface fastethernet 1/0**

R5(config-if)#**ip access-group LISTA-1 in**

R5(config-if)#**exit**

Paso 3: Configurar una ACL ampliada y nombrada en R3.

R3(config)#**ip access-list extended LISTA-2**

R3(config-ext-nacl)#**deny ip 192.168.2.0 0.0.0.255 host 200.200.200.100**

R3(config-ext-nacl)#**deny ip 192.168.2.0 0.0.0.255 host 200.200.200.200**

R3(config-ext-nacl)#**deny ip 192.168.2.0 0.0.0.255 host 200.200.200.400**

R3(config-ext-nacl)#**permit ip any any**

R3(config)#**interface serial 2/0**

R3(config-if)#**ip access-group LISTA-2 *out***

R3(config-if)#**exit**

R3(config)#**interface serial 2/1**

R3(config-if)#**ip access-group LISTA-2 out**

R3(config-if)#**exit**

R3(config)#**interface fastethernet 1/0**

R3(config-if)#**ip access-group LISTA-2 out**

R3(config-if)#**exit**

NOTA: Para verificar las ACL creadas en los routers colocar:

R1#**show ip access-list**

NOTA: Para eliminar la ACL colocar:

R5(config)#no **ip access-list standard LISTA-1**

R5(config)#**interface fastethernet 1/0**

R5(config-if)#**no ip access-group LISTA-1 in**

R5(config-if)#**exit**

De la misma manera se eliminan las ACL de los otros routers.

TAREA 6: CONFIGURAR LOS EQUIPOS DE HOST.

Configurar las direcciones IP y gateways por defecto como se indican en la tabla de direccionamiento de las interfaces Ethernet de C1, C2 (VPCS) y PC REAL.

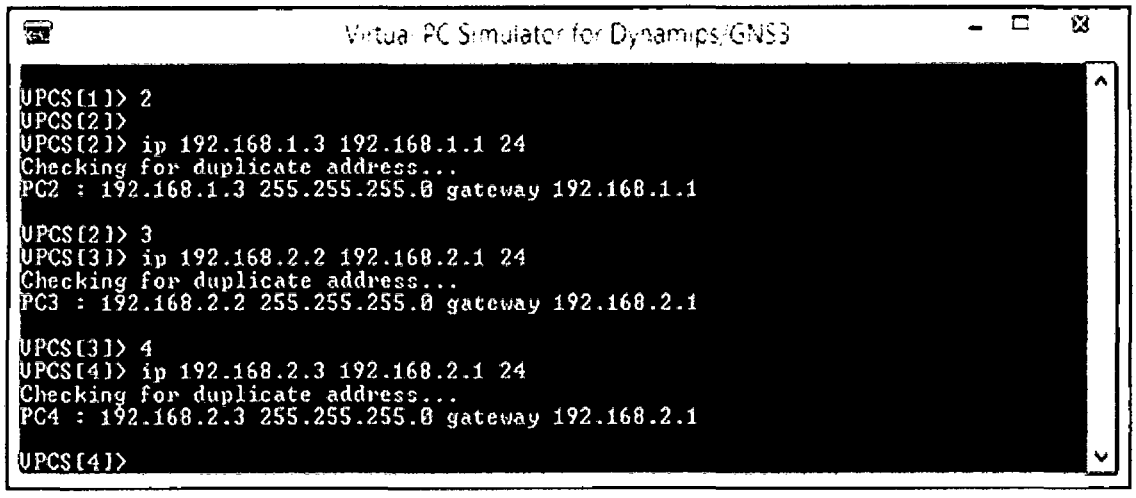


Fig. 4.14.2 Configuración de las direcciones IP en el VPCS.

TAREA 7: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

PASO 1: Verificar el direccionamiento IP y las interfaces.

R1#show ip interface brief

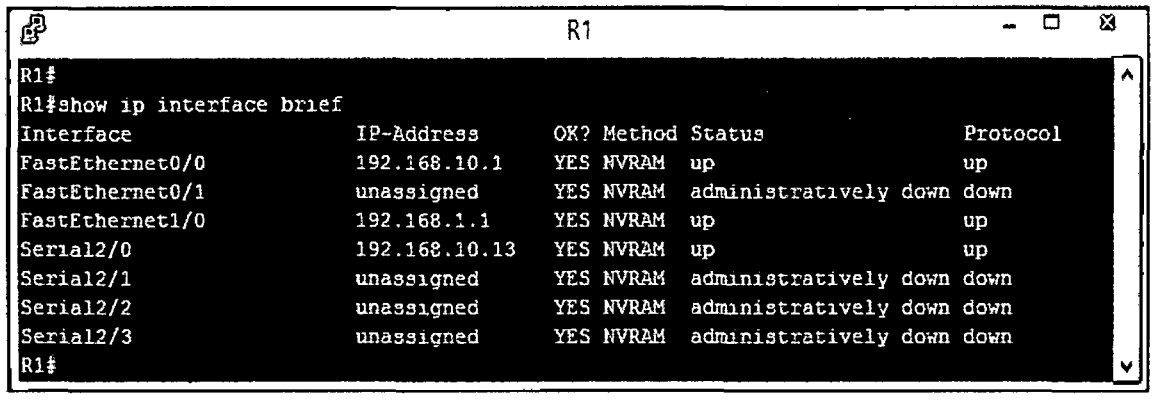


Fig. 4.14.3 Tabla ip de interface brief de R1.

NOTA: Verificar que las interfaces de los demás routers tengan la adecuada dirección IP y estén activas.

PASO 2: Verificar la configuración de los router. Use los comandos **show ip route** para verificar el contenido de la tabla de enrutamiento.

R2#show ip route

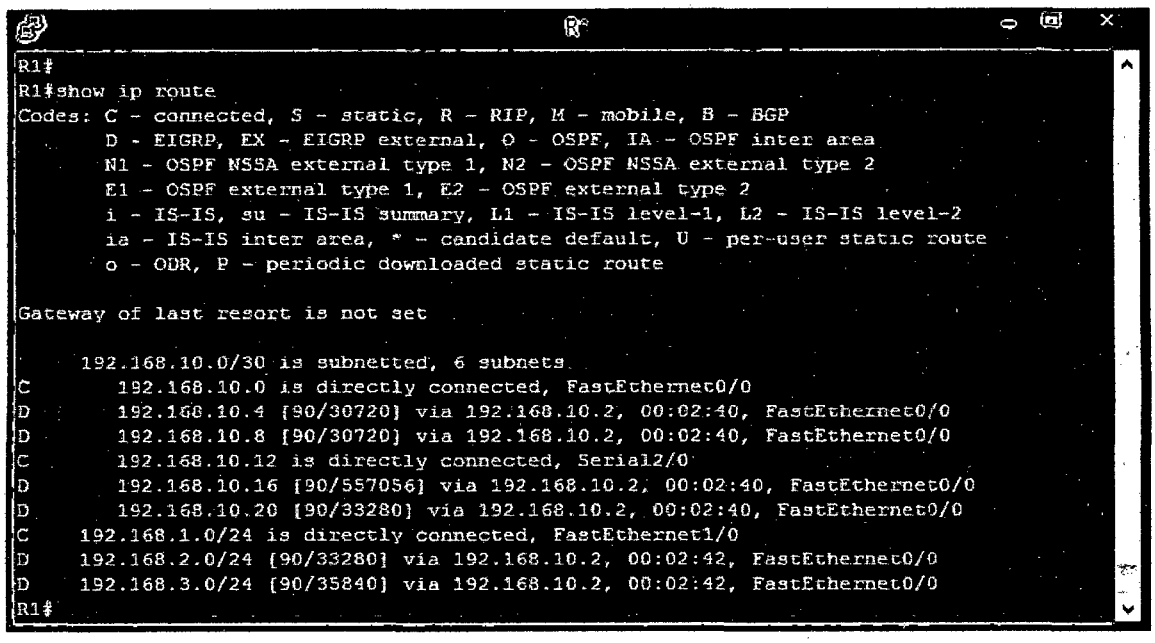


Fig. 4.14.4 Tabla de enrutamiento de R1.

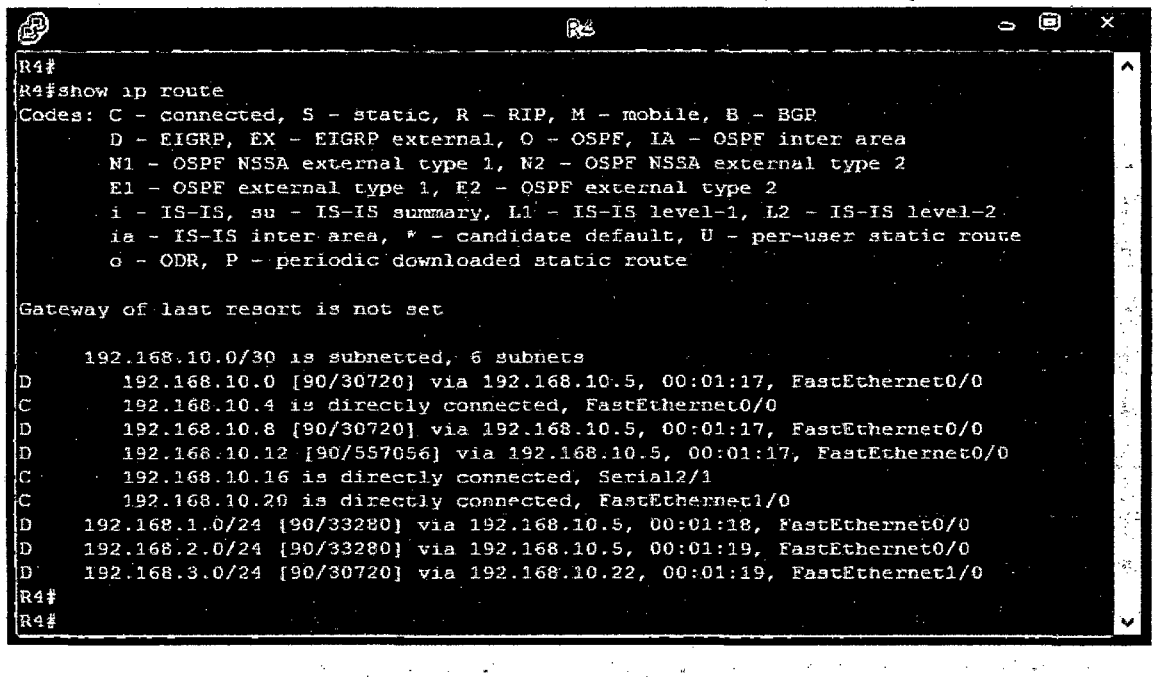


Fig. 4.14.5 Tabla de enrutamiento de R4.

NOTA: Verificar de igual manera la tabla de enrutamiento de los demás routers.

PASO 3: Verificar la configuración de la ACL con la ayuda del comando ping en el router configurado.

PASO 4: Verificar que hay conectividad completa en la red.

Use el comando **ping** para verificar la conectividad.

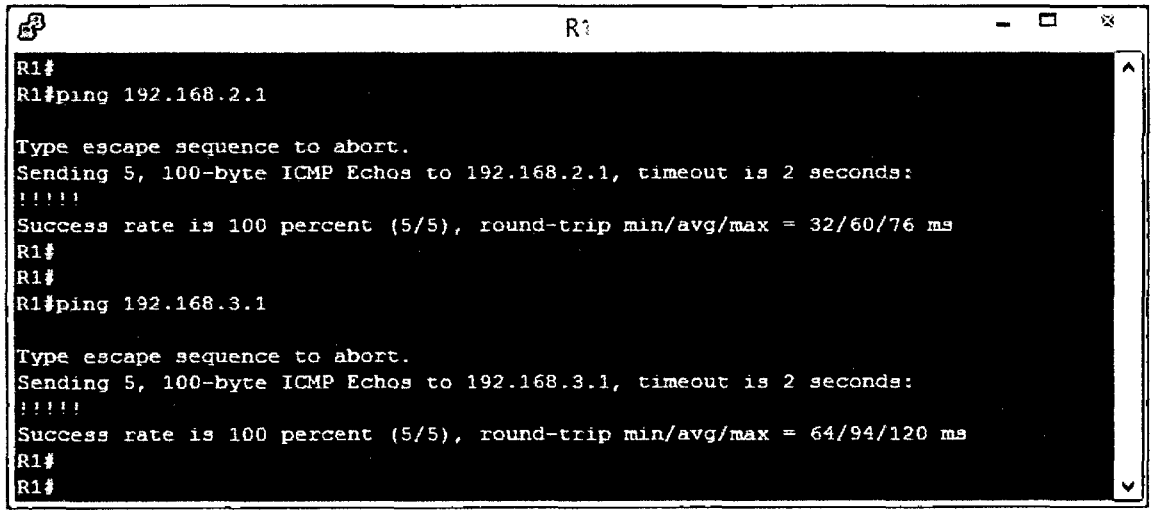


Fig. 4.14.6 Prueba de conectividad entre routers.

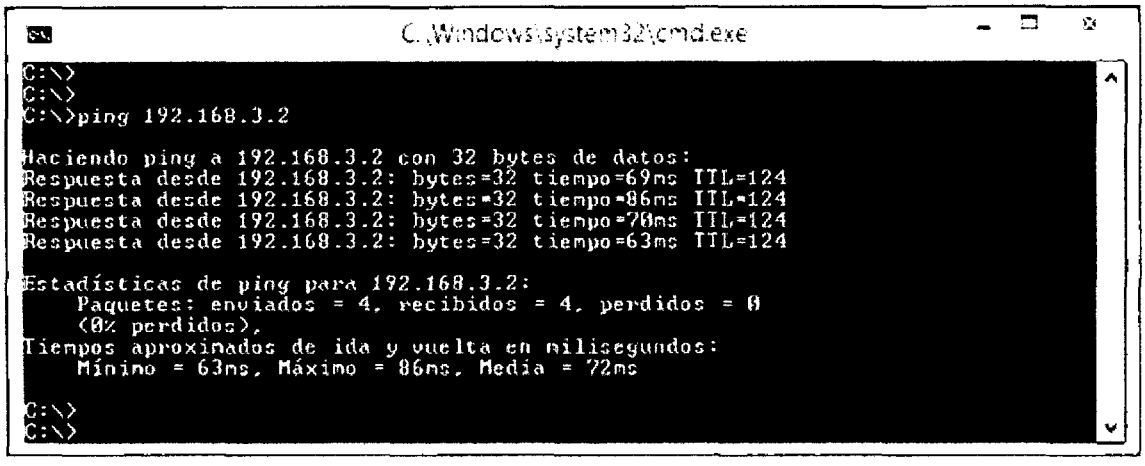


Fig. 4.14.7 Prueba de conectividad entre host desde C1 a PC real.

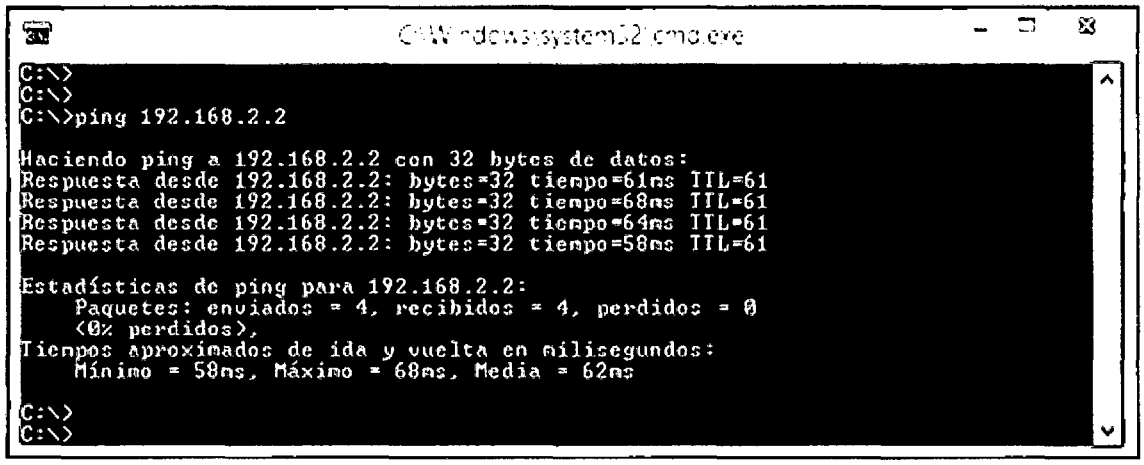


Fig. 4.14.8 Prueba de conectividad entre host desde C1 a C3.

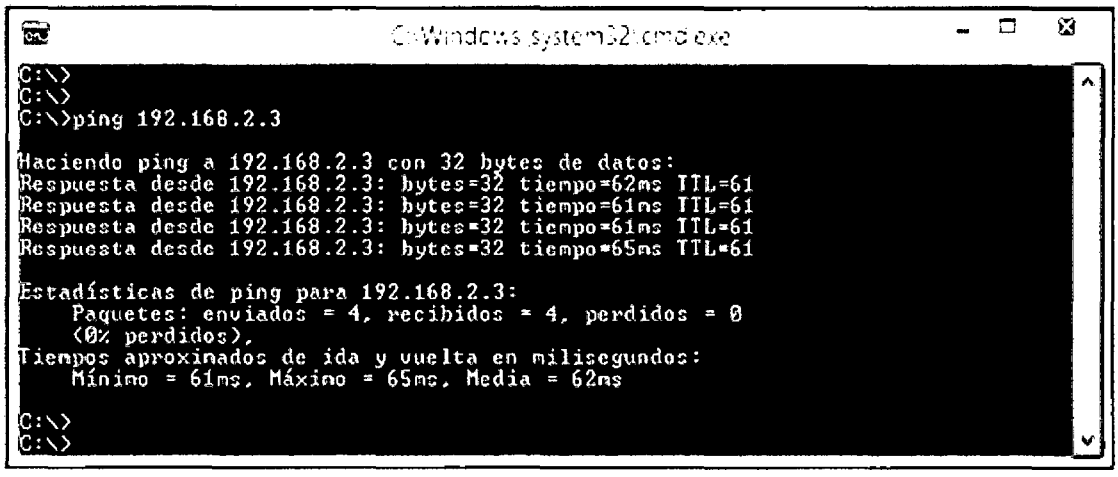


Fig. 4.14.9 Prueba de conectividad entre host desde C1 a C4.

TAREA 8: ANALISIS DEL TRAFICO DE PAQUETES

PASO 1: Medición de la Latencia

Para la medición de la latencia se realizó 10 muestras sucesivas de 100 ping desde el C1 (Bucle invertido) hacia la PC REAL considerando un tamaño de trama de 64, 512 y 1518 bytes como se especifica en el RFC 2544.

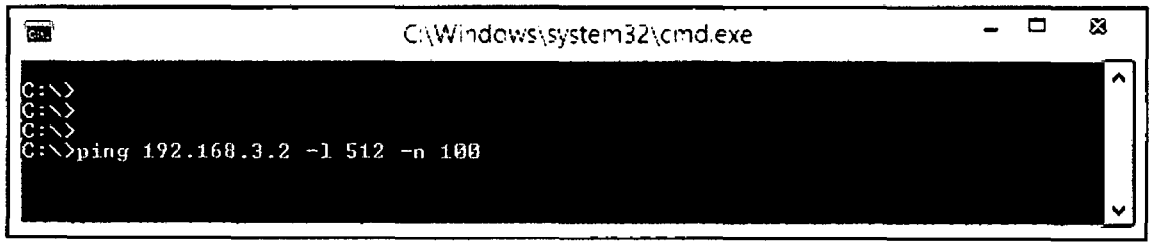


Fig. 4.14.10 Forma de medición de la latencia.

En la Figura 4.14.15 se puede observar el envío de 100 ping con una trama de 512 hacia la dirección 192.168.3.2

En las Tablas posteriores se detallan los valores de la Latencia que se ha obtenido una vez realizadas todas las muestras.

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	**60**	**55**	**56**	**56**	**60**	**56**	**54**	**61**	**62**	**59**	**57.9**
Tiempo Máximo (ms)	**349**	**239**	**266**	**276**	**343**	**281**	**208**	**406**	**412**	**303**	**308.3**
Tiempo Promedio (ms)	**113**	**103**	**109**	**108**	**113**	**114**	**98**	**119**	**124**	**111**	**111.2**

Tabla 4.14.2 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**512**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	**59**	**62**	**56**	**66**	**58**	**57**	**61**	**58**	**49**	**61**	**59.7**
Tiempo Máximo (ms)	**390**	**361**	**239**	**294**	**350**	**442**	**380**	**277**	**303**	**258**	**329.4**
Tiempo Promedio (ms)	**161**	**124**	**117**	**141**	**148**	**110**	**124**	**135**	**157**	**139**	**135.6**

Tabla 4.14.3 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**1518**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	**61**	**64**	**59**	**60**	**71**	**73**	**74**	**61**	**65**	**59**	**64.7**
Tiempo Máximo (ms)	**420**	**392**	**312**	**232**	**444**	**322**	**546**	**356**	**265**	**295**	**358.4**
Tiempo Promedio (ms)	**146**	**170**	**150**	**139**	**171**	**143**	**185**	**137**	**129**	**132**	**150.2**

Tabla 4.14.4 Datos obtenidos para una trama de 1518 bytes.

LATENCIA			
Tamaño de Trama (bytes)	**64**	**512**	**1518**
Tiempo Mínimo (ms)	**57.9**	**59.7**	**64.7**
Tiempo Máximo (ms)	**308.3**	**329.4**	**358.4**
Tiempo Promedio (ms)	**111.2**	**135.6**	**150.2**

Tabla 4.14.5 Comparación de datos obtenidos de las diferentes tramas.

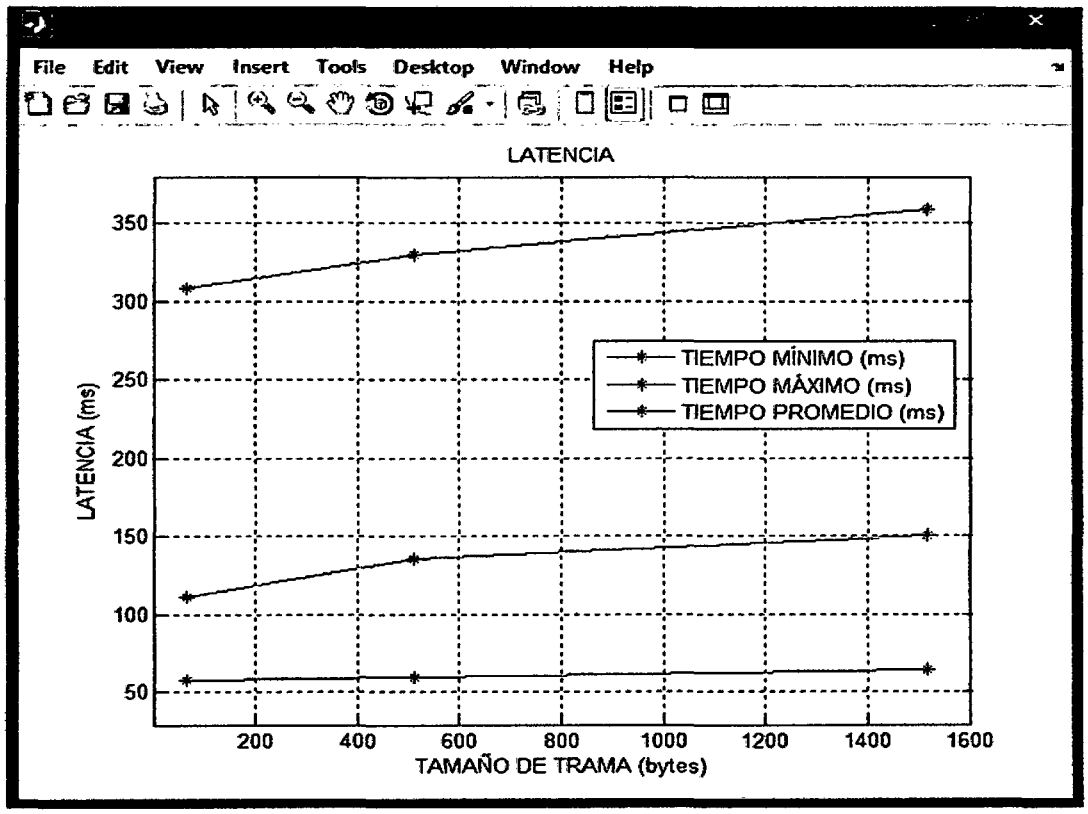


Fig. 4.14.11 Datos representados gráficamente de la variación de la latencia.

De acuerdo con los datos obtenidos, se puede observar claramente que los valores mínimo (color azul), máximo (color rojo) y promedio (color verde) de la latencia de la red se incrementan conforme se envía una trama de longitud mayor, en este caso con la trama de 1518 bytes se obtiene una latencia promedio de 150.2 ms a diferencia de una trama de 64 bytes con 111.2 ms.

PASO 2: Medición del Throughput

Para la medición del Throughput y Jitter se envió una cantidad de tramas a velocidades diferentes durante 20 segundos, hasta encontrar la máxima cantidad de tramas recibidas sin que se produzcan perdidas de las mismas en el router y PC REAL. Como se utilizó Jperf el cliente será el encargado de enviar los paquetes y el servidor los recibirá, indicando la cantidad de paquetes que llegaron correctamente considerando un tamaño del paquete UDP de 750, 1125, 1500 y 1470 (default) bytes, tal como se especifica en el RFC 768.

Configuración del Jperf como servidor para medir Throughput:

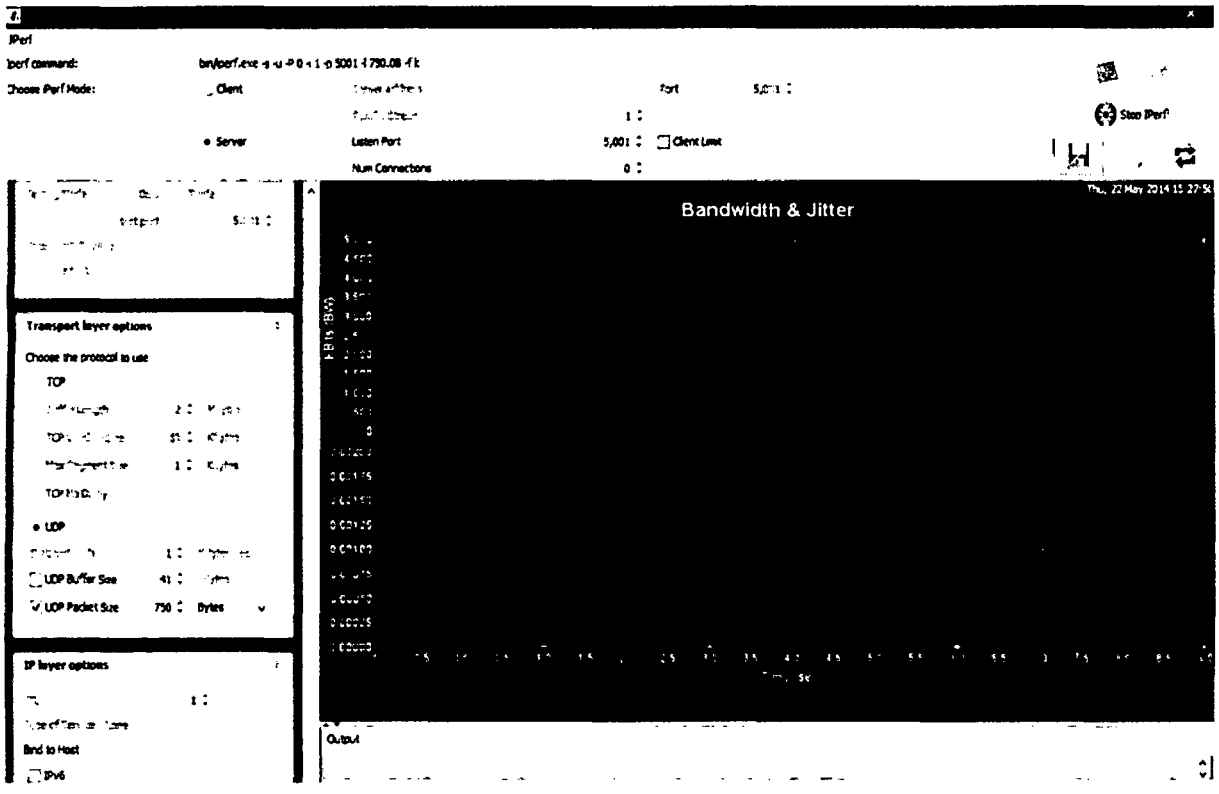


Fig. 4.14.12 Gráfica de Bandwidth y Jitter

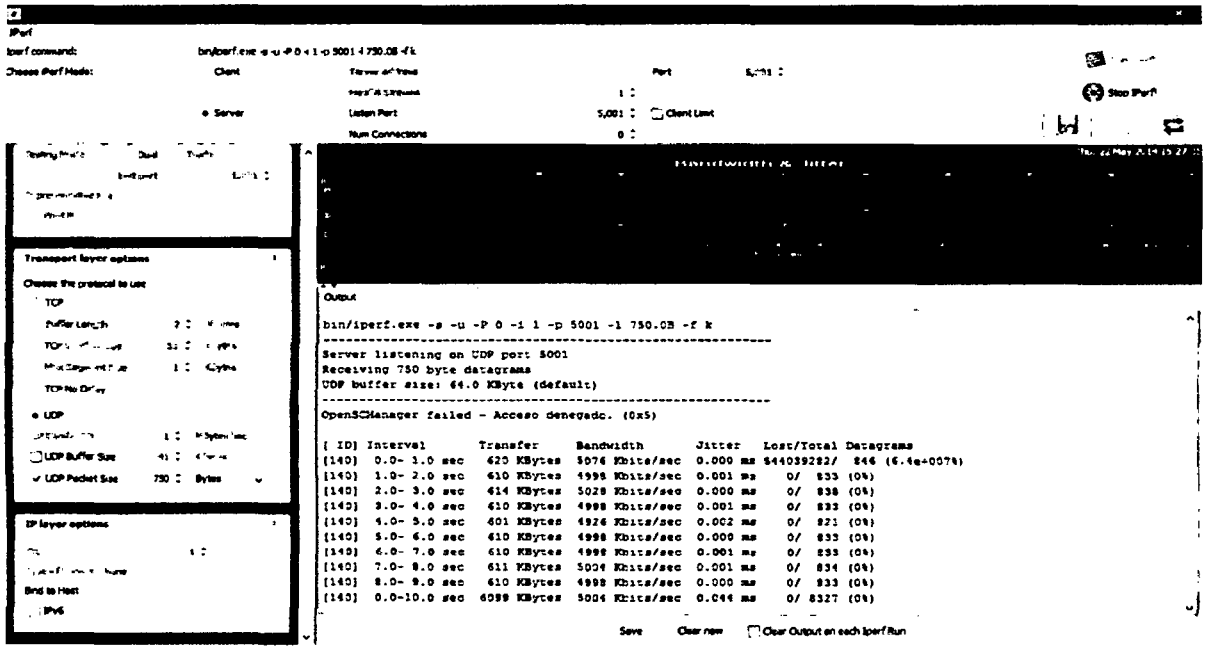


Fig. 4.14.13 Resultados al medir Throughput como servidor.

Configuración del Jperf como cliente para medir Throughput:

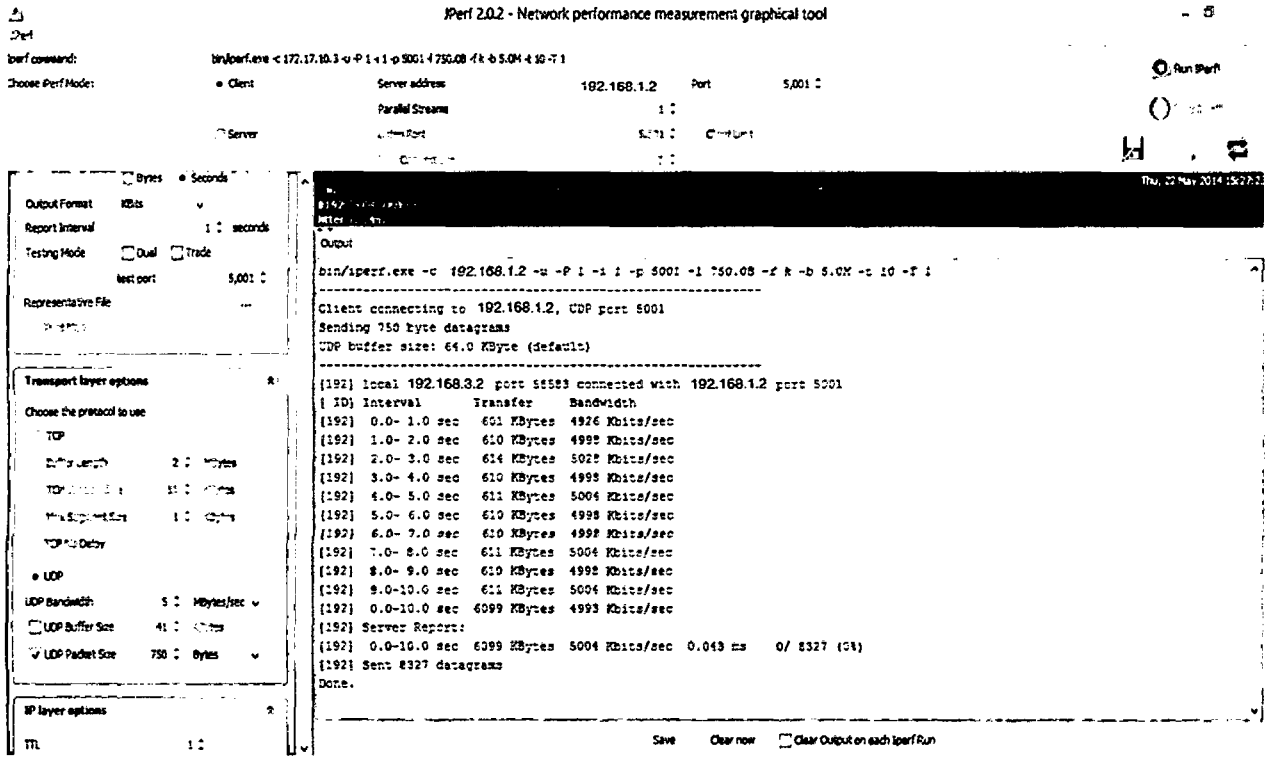


Fig. 4.14.14 Resultados del Jperf como Cliente al medir Throughput.

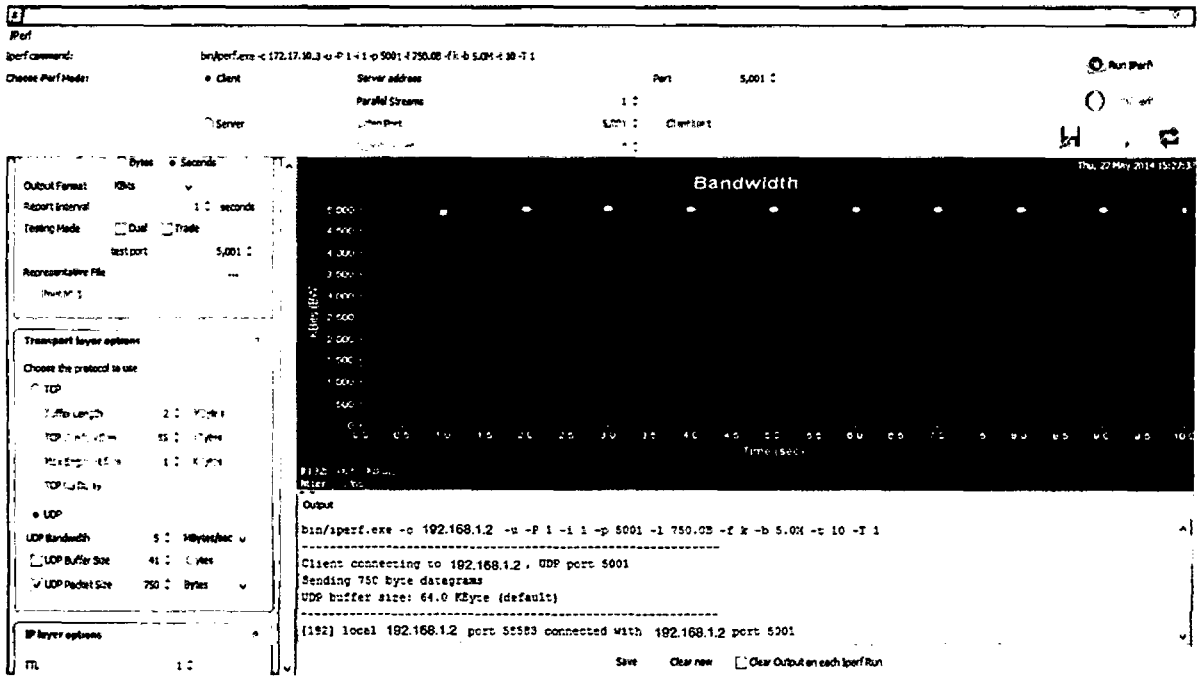


Fig. 4.14.15 Gráfica de Bandwidth

En las siguientes Tablas se detalla los valores del Throughput obtenidos una vez realizada todas las muestras.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**5**	**5**	**5**
Velocidad de Rx (Mbps)	**5**	**5**	**5**
Tramas Transmitidas	**8329**	**5549**	**4165**
Tramas Recibidas	**8329**	**5549**	**4165**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**832**	**555**	**416**

Tabla 4.14.6 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**1**	**5**	**8**	**10**
Velocidad de Rx (Mbps)	**0.99**	**4.99**	**7.99**	**10**
Tramas Transmitidas	**851**	**4249**	**6796**	**8497**
Tramas Recibidas	**851**	**4249**	**6796**	**8497**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**85**	**424**	**680**	**850**

Tabla 4.14.7 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

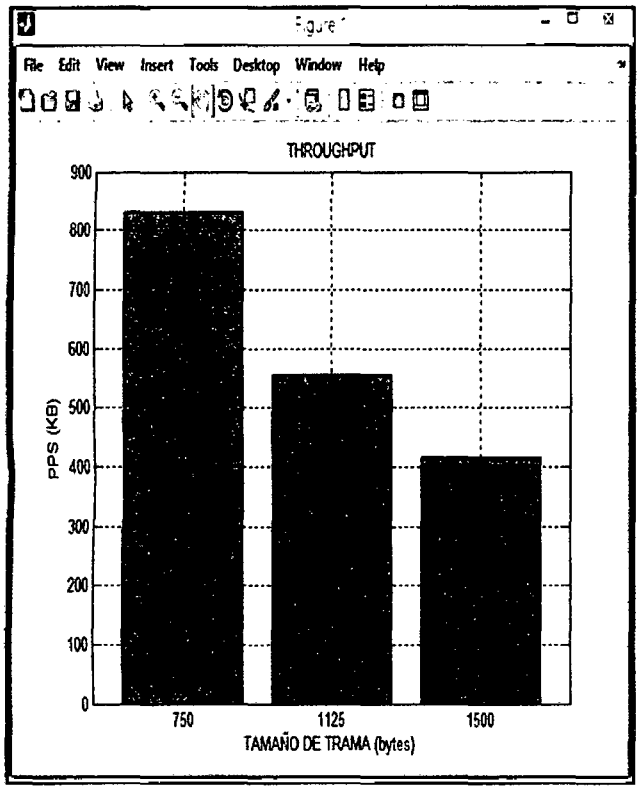


Fig. 4.14.16 PPS vs. Tamaño de Trama.

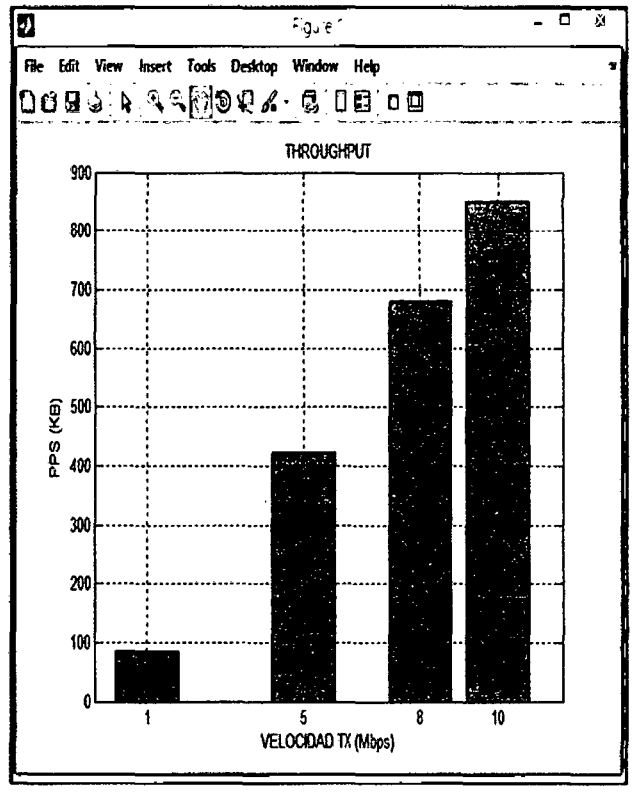


Fig. 4.14.17 PPS vs. Velocidad Tx.

En la figura 4.14.16, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 750 bytes, 1125 bytes y 1500 bytes los cuales han utilizado una velocidad de Tx constante de 5 Mbps, en la gráfica se puede observar claramente que al enviar una trama de 750 bytes se envía 832 pps, con una trama de 1125 se envía 555 pps y con una trama de 1500 se envía 416 pps.

Mientras en la figura 4.14.17, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 1470 bytes los cuales han utilizado una velocidad de Tx variada de: 1 Mbps, 5 Mbps, 8 Mbps y 10 Mbps, sin que se produzcan perdidas en el envío, como los datos que se muestran en la tabla 4.14.7.

PASO 3: Medición del Jitter

Para la medición se envió datos UDP de longitud variable a velocidades diferentes de Throughput obtenida anteriormente durante 20 segundos. Como se utilizó anteriormente Jperf el cliente será el encargado de enviar los datos y el servidor los recibirá, indicando los valores de Jitter obtenidos durante la transmisión de los datos.

JITTER			
Longitud de Trama (bytes)	750	1125	1500
Velocidad de Tx (Mbps)	5	5	5
Velocidad de Rx (Mbps)	5	5	5
Tramas Transmitidas	8329	5549	4165
Tramas Recibidas	8329	5549	4165
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	0.004	0.001	0.001

Tabla 4.14.8 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER				
Longitud de Trama (bytes)	1470	1470	1470	1470
Velocidad de Tx (Mbps)	1	5	8	10
Velocidad de Rx (Mbps)	0.99	4.99	7.99	10
Tramas Transmitidas	851	4249	6796	8497
Tramas Recibidas	851	4249	6796	8497
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	1.104	0	0	0

Tabla 4.14.9 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

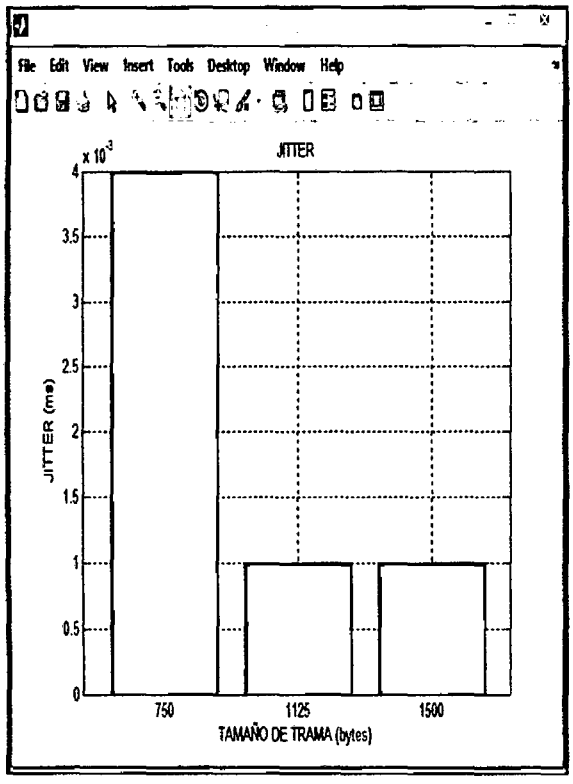


Fig. 4.14.18 Jitter vs. Tamaño de Trama

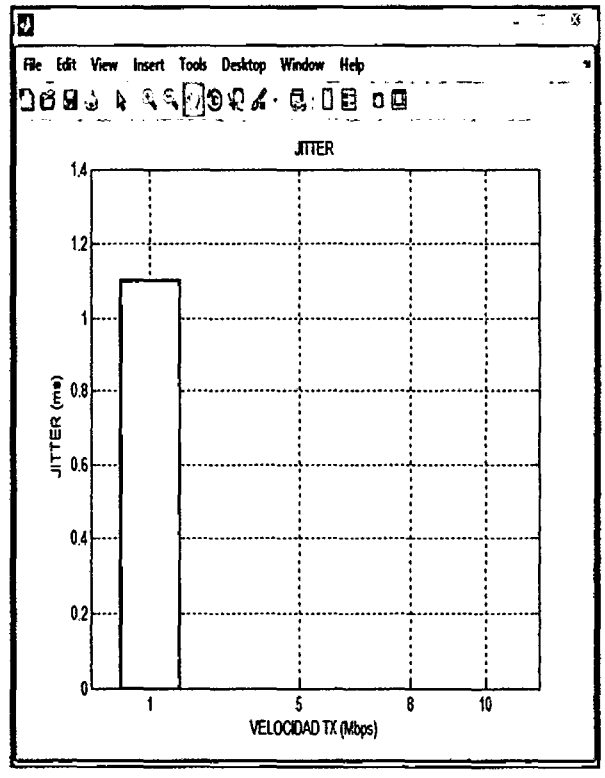


Fig. 4.14.19 Jitter vs. Velocidad Tx

En la figura 4.14.18 se observa los valores del Jitter obtenidos al enviar diferentes tamaños de paquete UDP como 750, 1125 y 1500 bytes utilizando una velocidad de Tx constante de 5 Mbps, se puede observar claramente que con una trama de 750 bytes se tiene un Jitter de 0.104 ms a diferencia de la trama de 1500 bytes en la cual se tiene un Jitter de 0 ms.

En la figura 4.14.19, se observa los valores del Jitter obtenidos al enviar paquetes UDP de 1470 bytes utilizando una velocidad de Tx que varía entre 1 Mbps, 5 Mbps, 8 Mbps y 10 Mbps sin que se pierdan paquetes en la red, concluyendo también que a mayor ancho de banda mucho mayor será el jitter y pérdidas de datagramas.

Medición de Jitter a 2 Mbps:

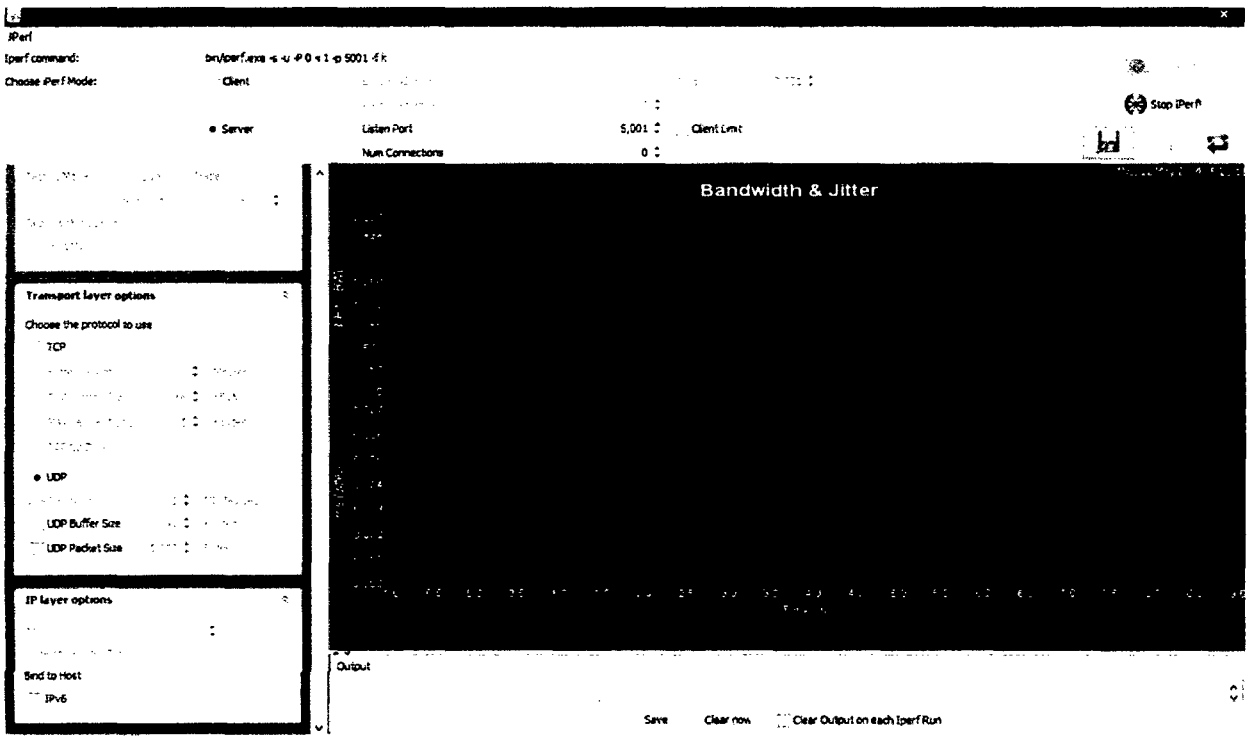


Fig. 4.14.20 Gráfica de Bandwidth y Jitter.

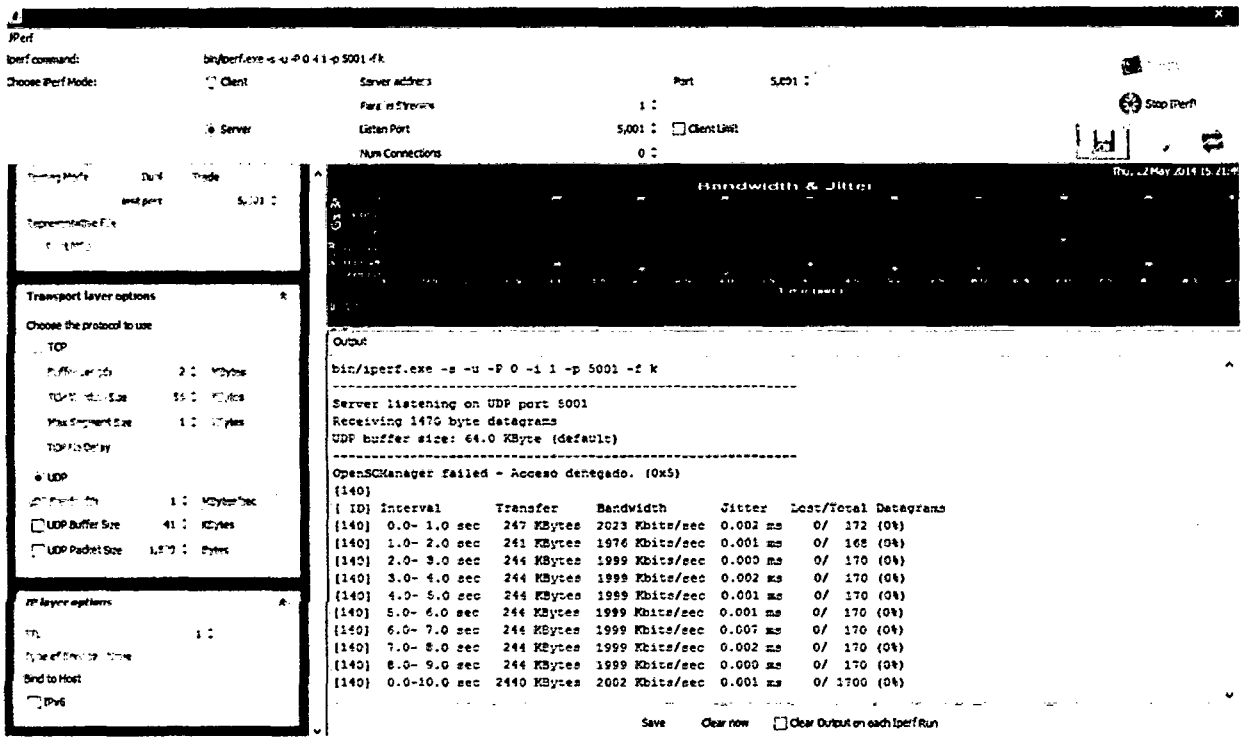


Fig. 4.14.21 Resultados al medir Throughput como servidor.

PASO 4: Captura de tráfico con Wireshark.

Capturar tráfico de paquetes en la interfaz s1/3 de R1.

- Captura de paquetes ICMP.

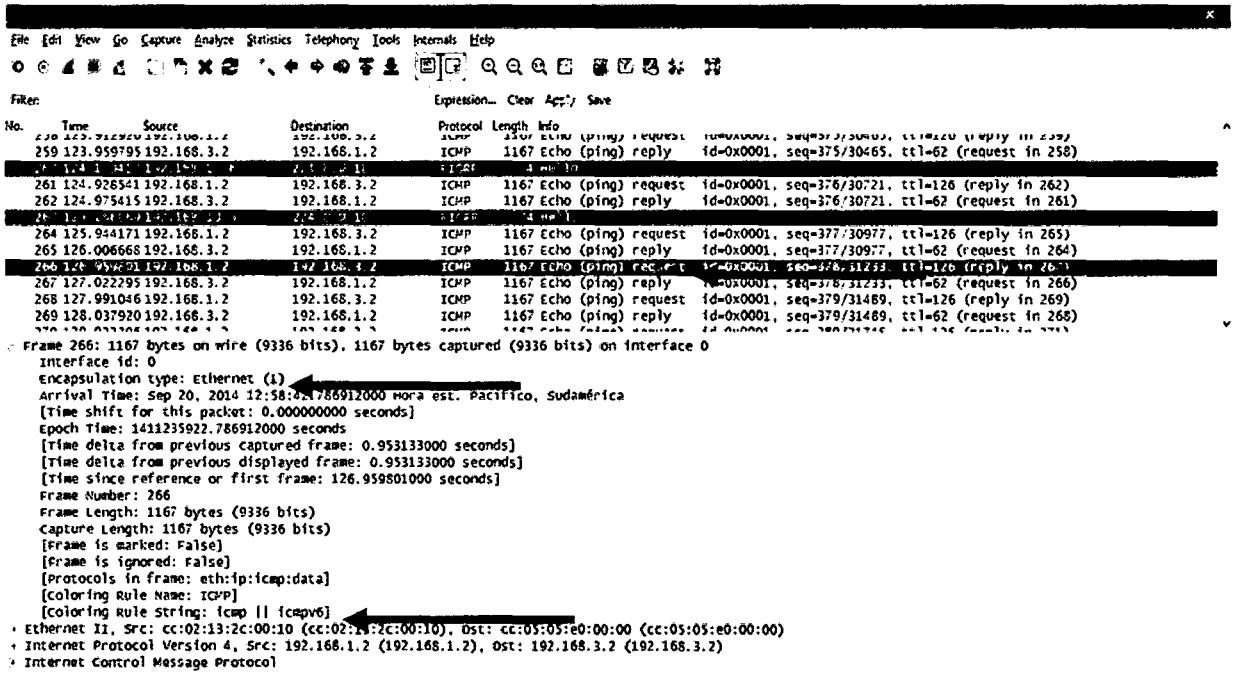


Fig. 4.14.22 Captura de paquetes ICMP con Wireshark.

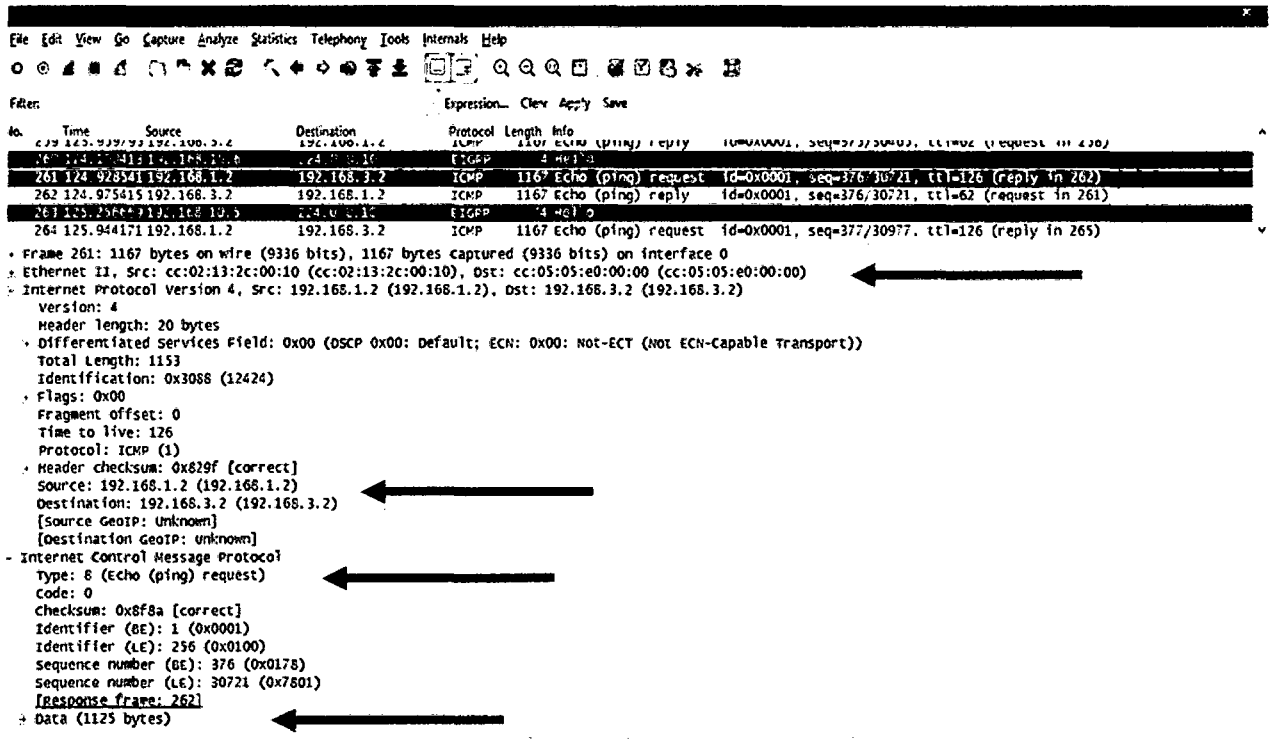


Fig. 4.14.23 Información detallada del origen y destino de paquetes.

- Protocolo de enrutamiento EIGRP:

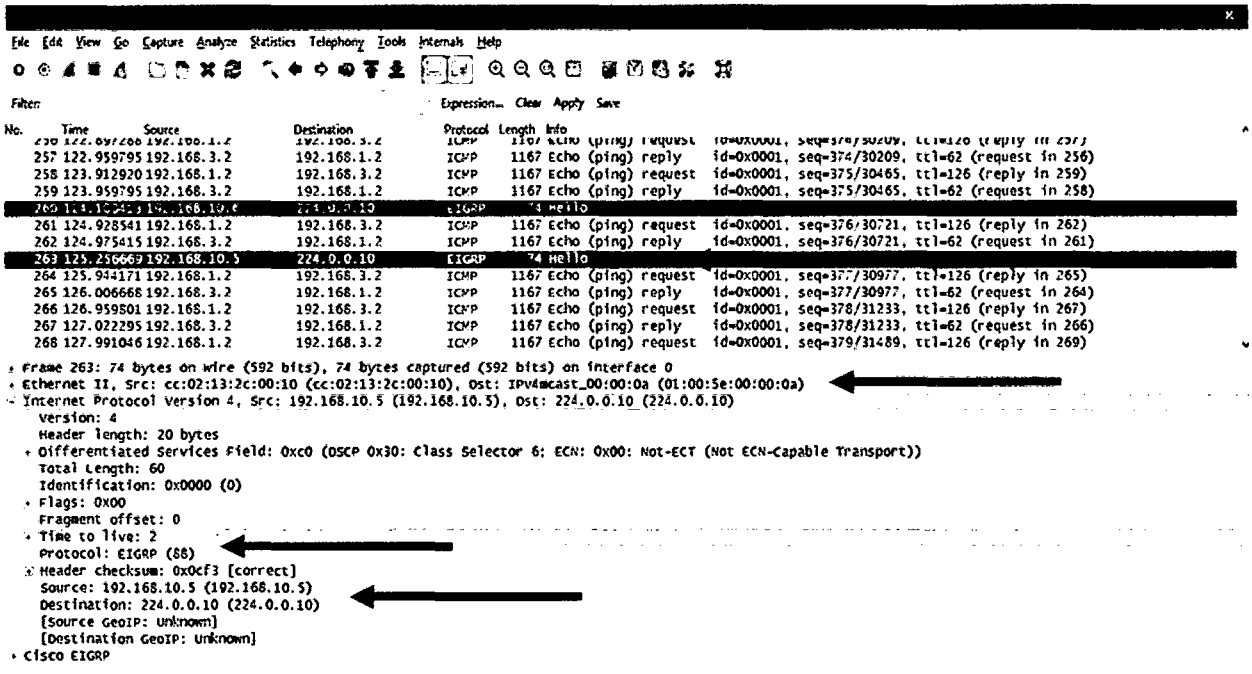


Fig. 4.14.24 Captura del protocolo de enrutamiento EIGRP con wireshark.

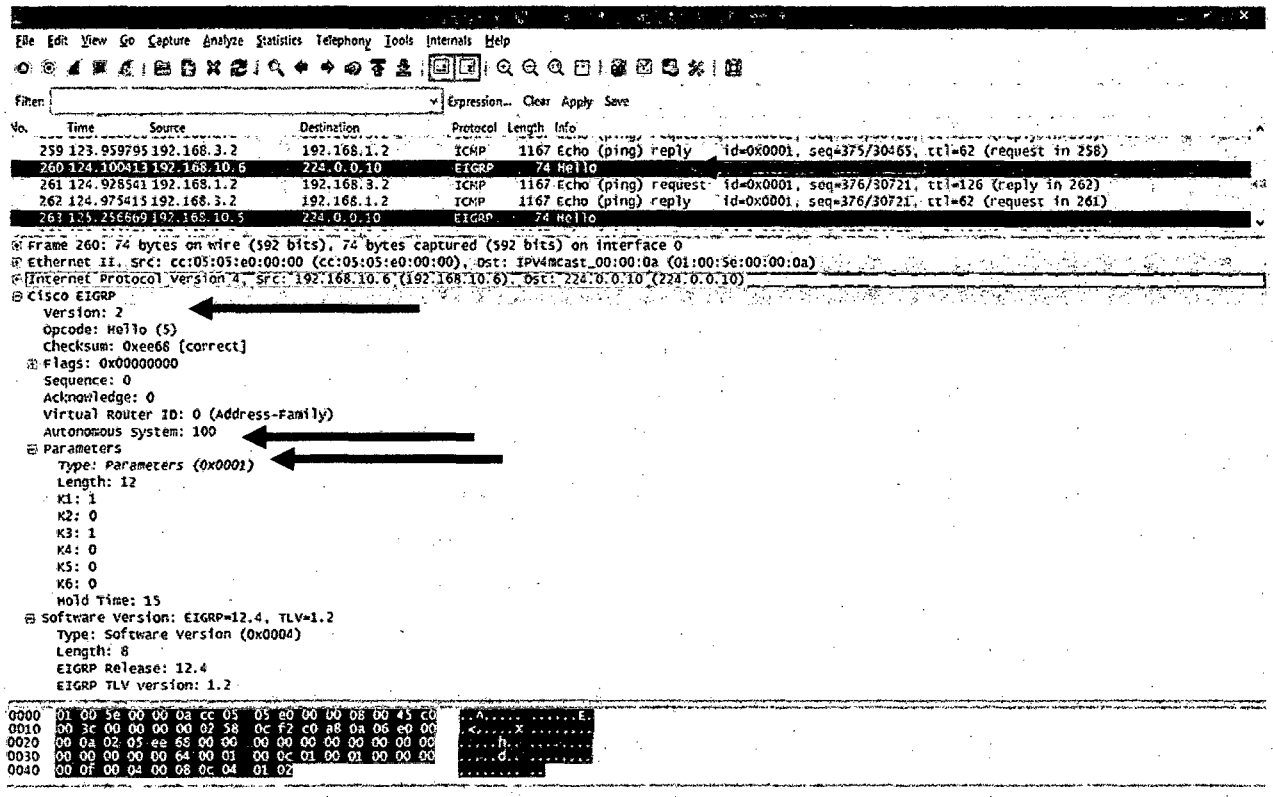


Fig. 4.14.25 Información detallada del protocolo EIGRP.

LABORATORIO 4.15: ASA FIREWALL

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet.
- Configurar ASA Firewall.
- Configurar ASDM.
- Enrutamiento estático y por defecto.
- Probar la conectividad.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **40.0.0.0/8** entre R1-ASA, **50.0.0.0/16** entre ASA-R2, **41.0.0.0/8** entre R1-R4, **42.0.0.0/8** entre R1-R3, además teniendo los siguientes requisitos:

LAN R3: 192.168.1.0/24
LAN R4: 192.168.1.0/24

DIAGRAMA DE TOPOLOGIA

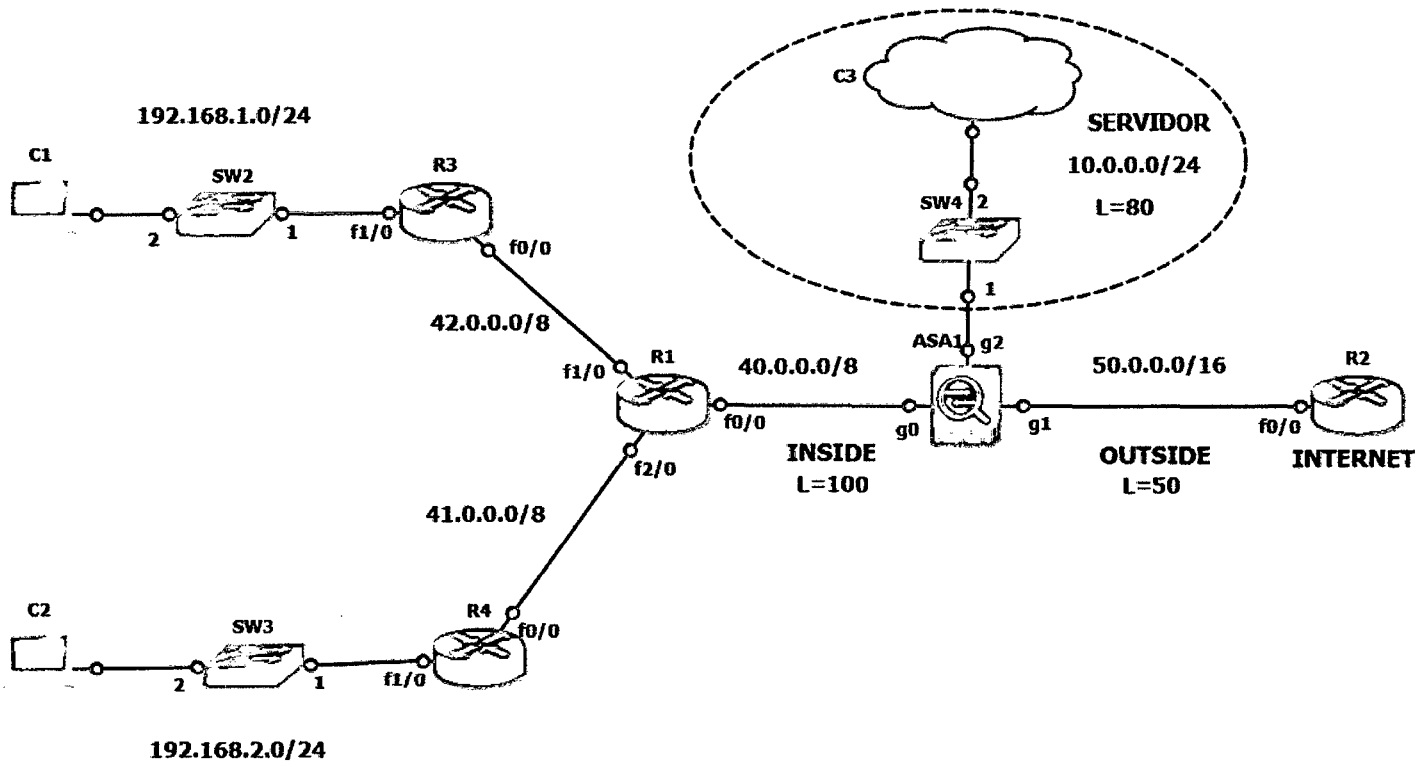


Fig. 4.15.1 Red Virtual en GNS3

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	f0/0	40.0.0.2	255.0.0.0	No aplicable
	f1/0	42.0.0.1	255.0.0.0	No aplicable
	f2/0	41.0.0.1	255.0.0.0	No aplicable
R2	f0/0	50.0.0.2	255.255.0.0	No aplicable
R3	f0/0	42.0.0.2	255.0.0.0	No aplicable
	f1/0	192.168.1.1	255.255.255.0	No aplicable
R4	f0/0	41.0.0.2	255.0.0.0	No aplicable
	f1/0	192.168.2.1	255.255.255.0	No aplicable
C1	VPCS	192.168.1.2	255.255.255.0	192.168.1.1
C2	VPCS	192.168.2.2	255.255.255.0	192.168.2.1
C3	BUCLE INVERTIDO	10.0.0.3	255.255.255.0	10.0.0.1

Tabla 4.15.1 Direccionamiento IP para las Redes

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

Montar y conectar la red igual a la del Diagrama de topología.

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

Ingrese al modo privilegiado

Router>enable

Aparece el siguiente prompt

Router#

En el modo exec privilegiado, ingrese al modo de configuración global:

Router# **configure terminal**

PASO 1: Establezca la configuración global del nombre de host.

Ingrese el siguiente comando para configurar el nombre del router:

Router(config)#**hostname XXXXXX** (Escribir nombre deseado)

PASO 2: Desactive la búsqueda DNS.

Router(config)# **no ip-domain lookup**

Si escribes algo que no sea un comando de Cisco IOS o cometes un error, el router asume que ha escrito un nombre de dominio y trata de resolver lo que usted escribe, realizando una búsqueda de DNS.

PASO 3: Configure un mensaje para que se muestre al ingresar al router.

Router(config)#**banner motd %** Solo acceso a personal autorizado **%** (Puede escribir cualquier mensaje)

El símbolo % indica el inicio y final del mensaje.

PASO 4: Configure las contraseñas de consola, enable secret y VTY.

Seguir los siguientes pasos:

Router(config)# **line console 0**

Router(config-line)# **password XXXXX** (Escribir contraseña deseada)

Router(config-line)# **login**

Router(config-line)# **exit**

Router(config)# **enable secret XXXXX** (Escribir contraseña deseada)

Router(config)# **line vty 0 4**

Router(config-line)# **password XXXXX** (Escribir contraseña deseada)

Router(config-line)# **login**

Router(config-line)# **exit**

PASO 5: Sincronice los mensajes no solicitados y el resultado de la depuración con el resultado solicitado y los indicadores para las líneas de consola y de terminal virtual.

Router(config)# **line console 0**

Router(config)# **logging synchronous**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **logging synchronous**

Router(config)# **exit**

PASO 6: Configure un tiempo de espera EXEC de 10 minutos.

Router(config)# **line console 0**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

PASO 7: Guardar la configuración.

Router(config)# **copy running-config startup-config**

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES FASTETHERNET.

R1:

R1(config)# **interface fasEthernet 0/0**

R1(config-if)# **description conexion a ASA_FIREWALL**

R1(config-if)# **ip address 40.0.0.2 255.0.0.0**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface fasEthernet 1/0**

R1(config-if)# **description conexion a R3**

R1(config-if)# **ip address 42.0.0.1 255.0.0.0**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface fasEthernet 2/0**

R1(config-if)# **description conexion a R4**

R1(config-if)# **ip address 41.0.0.1 255.0.0.0**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

NOTA: Seguir los mismos pasos para las demás routers con sus respectivos parámetros.

TAREA 4: CONFIGURAR ASA FIREWALL.

ASA1(config)# **interface gigabitEthernet 0**

ASA1(config-if)# **ip address 40.0.0.1 255.0.0.0**

ASA1(config-if)# **no shutdown**

ASA1(config-if)# **nameif INSIDE**

ASA1(config-if)# **exit**

ASA1(config)# **interface gigabitEthernet 1**

ASA1(config-if)# **ip address 50.0.0.1 255.255.0.0**

ASA1(config-if)# **no shutdown**

ASA1(config-if)# **nameif OUTSIDE**

ASA1(config-if)# **security-level 50**

ASA1(config-if)# **exit**

ASA1(config)# **interface gigabitEthernet 2**

ASA1(config-if)# **ip address 10.0.0.1 255.255.255.0**

ASA1(config-if)# **no shutdown**

ASA1(config-if)# **nameif DMZ**

ASA1(config-if)# **security-level 80**

ASA1(config-if)# **exit**

TAREA 5: CONFIGURAR CISCO ADAPTIVE SECURITY MANAGER (ASDM).

PASO 1: Descargar el software Tftpd32, ejecutar y seleccionar en **Server interfaces** la red de bucle invertido, la cual está configurada con la IP 10.0.0.3 255.255.255.0 GW: 10.0.0.1

PASO 2: Configurar en ASA los siguientes pasos:

ASA1# **copy tftp flash:**

Address or name of remote host [ ] ? **10.0.0.3**

Source filename host [ ] ? **asdm-712.bin**

Destination filename [asdm-712.bin] ? **Presionar Enter**

Empezará a cargar, tal como se muestra en la siguiente figura:

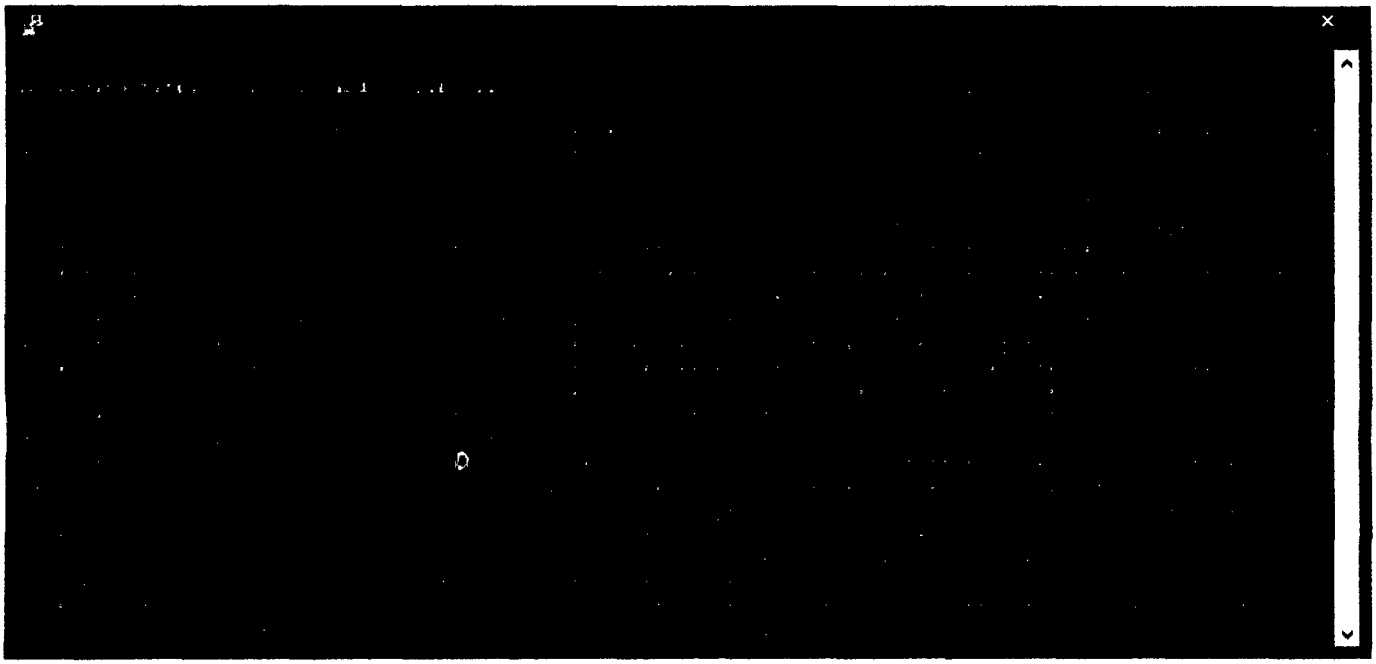


Fig. 4.15.2 Cargando Tftp

Luego:

ASA1# **configure terminal**

ASA1(config)# **asdm image flash: asdm-712.bin**

ASA1(config)# **http server enable**

ASA1(config)# **http 10.0.0.0 255.255.255.0 DMZ**

ASA1(config)# **username unprg password cisco privilege 15**

ASA1(config)# **exit**

TAREA 6: REALIZAR ENRUTAMIENTO ESTATICO.

ASA1:

ASA1(config)# **route INSIDE 41.0.0.0 255.0.0.0 40.0.0.2**

ASA1(config)# **route INSIDE 42.0.0.0 255.0.0.0 40.0.0.2**

ASA1(config)# **route INSIDE 192.168.1.0 255.255.255.0 40.0.0.2**

ASA1(config)# **route INSIDE 192.168.2.0 255.255.255.0 40.0.0.2**

R1:

R1(config)# **ip route 0.0.0.0 0.0.0.0 40.0.0.1**

R1(config)# **ip route 192.168.1.0 255.255.255.0 42.0.02**

R1(config)# **ip route 192.168.2.0 255.255.255.0 41.0.02**

R2:

R2(config)# **ip route 0.0.0.0 0.0.0.0 50.0.0.1**

NOTA: Seguir los mismos pasos para las demás routers con sus respectivos parámetros.

TAREA 6: CONFIGURAR LOS EQUIPOS DE HOST.

VPCS

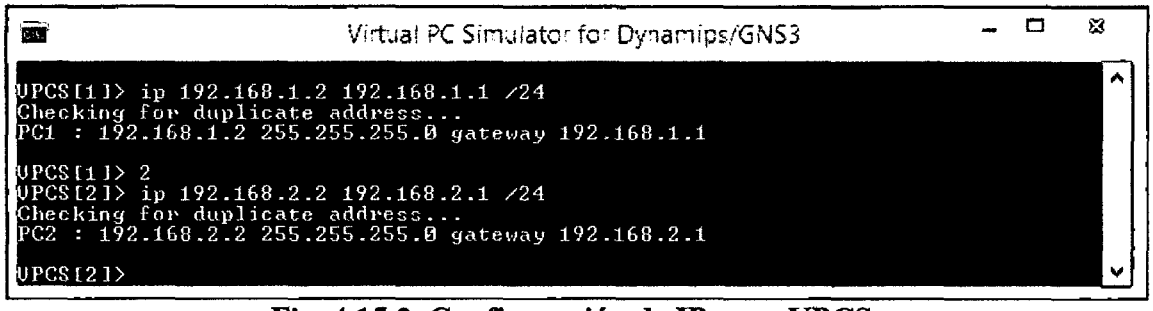


Fig. 4.15.3 Configuración de IP para VPCS.

BUCLE INVERTIDO

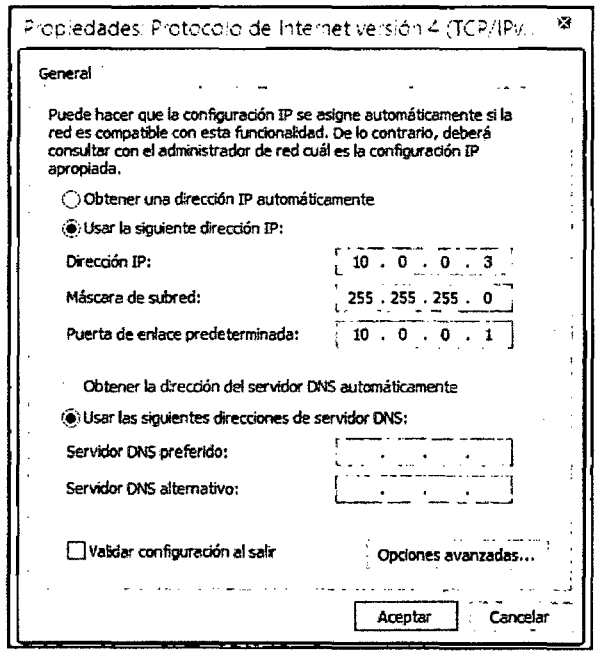


Fig. 4.15.4 Configuración de IP para BUCLE INVERTIDO.

TAREA 7: VERIFICAR FUNCIONAMIENTO DE ASA FIREWALL.

PASO 1: La configuración realizada anteriormente, no permite que se realice ping entre los routers de la INDISE hacia la OUTSIDE y en viceversa, como se observan en las imágenes:

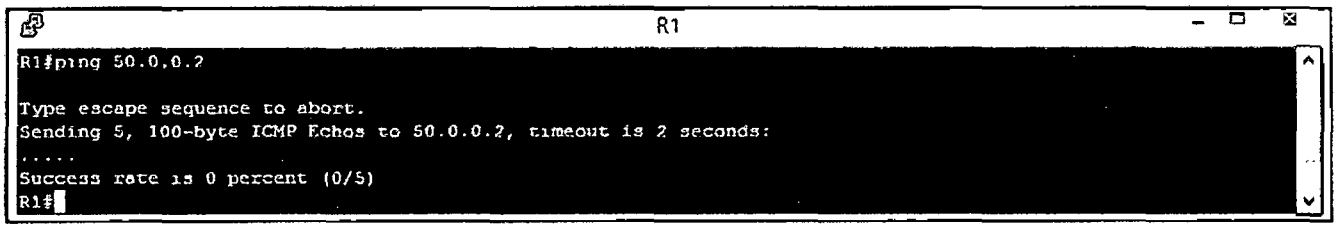


Fig. 4.15.5 Prueba de conectividad a R2.

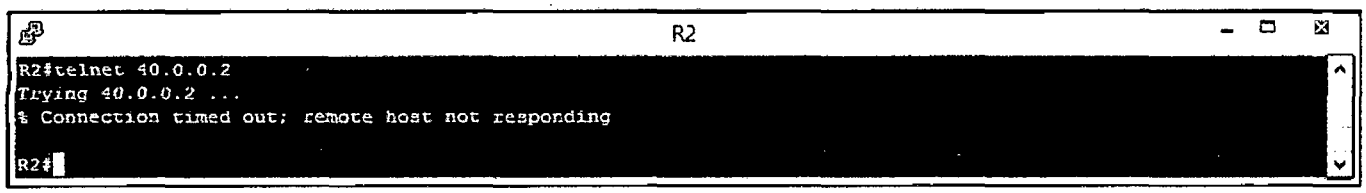


Fig. 4.15.6 Prueba de conectividad a R1.

Pero si permite que cualquier router de la INSIDE puede conectarse a un router de la OUTSIDE mediante telnet, y la vez no permite que cualquier router de la OUTSIDE pueda conectarse por telnet a cualquier router INSIDE debido a que tiene seguridad de 100, como se observan en las imágenes:

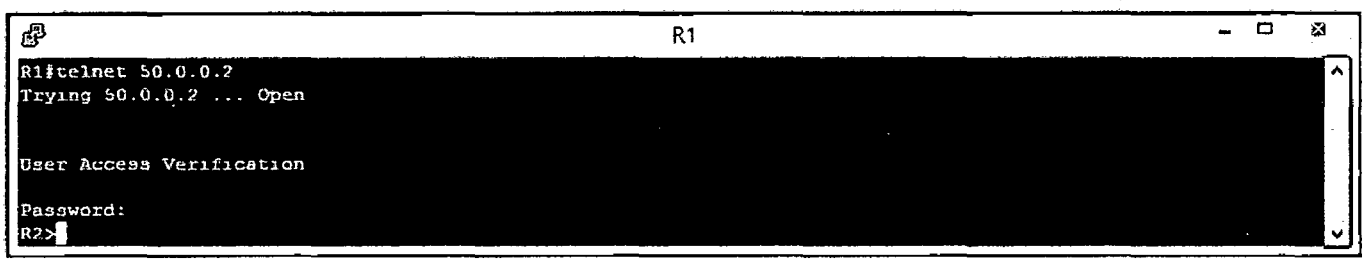


Fig. 4.15.7 Prueba de telnet a R2.

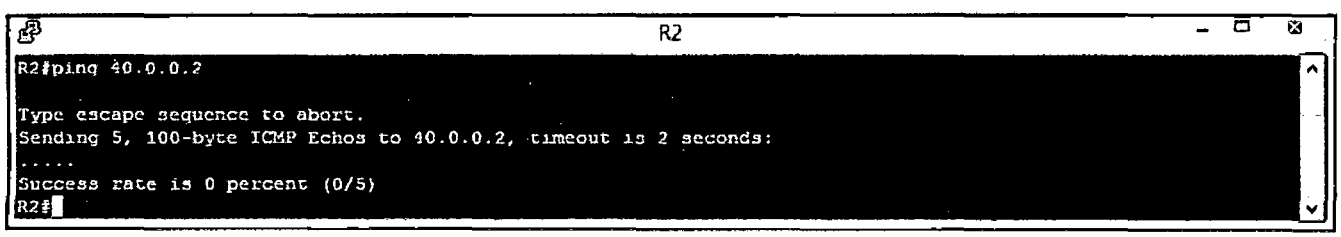


Fig. 4.15.8 Prueba de telnet a R1.

Para poder realizar ping entre la red INSIDE hacia la OUTSIDE o viceversa, se deben crear ACL, siguiendo los siguientes pasos:

ASA1# **configure terminal**

ASA1(config)# **access-list unprg permit icmp any any**

ASA1(config)# **access-group unprg in interface OUTSIDE**

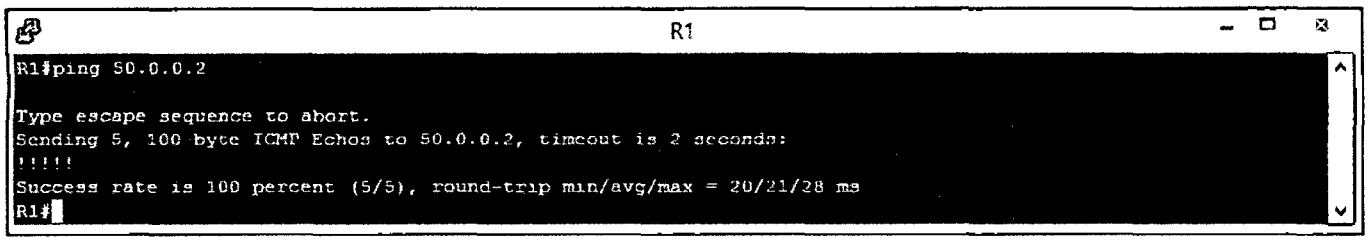


Fig. 4.15.9 Prueba de conectividad a R2.

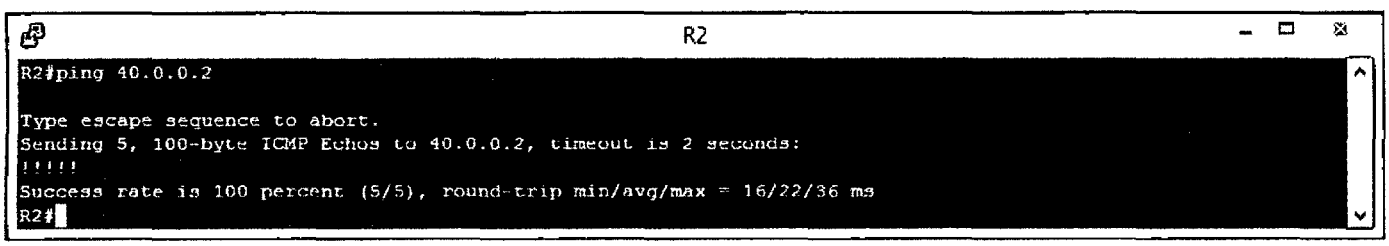


Fig. 4.15.10 Prueba de conectividad a R1.

Ahora solo permitiremos que la red INSIDE pueda hacer ping a la OUTSIDE:

ASA1# **configure terminal**

ASA1(config)# ***no access-list unprg permit icmp any any***

ASA1(config)# **access-list unprg permit icmp any any echo-reply**

ASA1(config)# **access-group unprg in interface OUTSIDE**

Podremos observar las imágenes, los resultados:

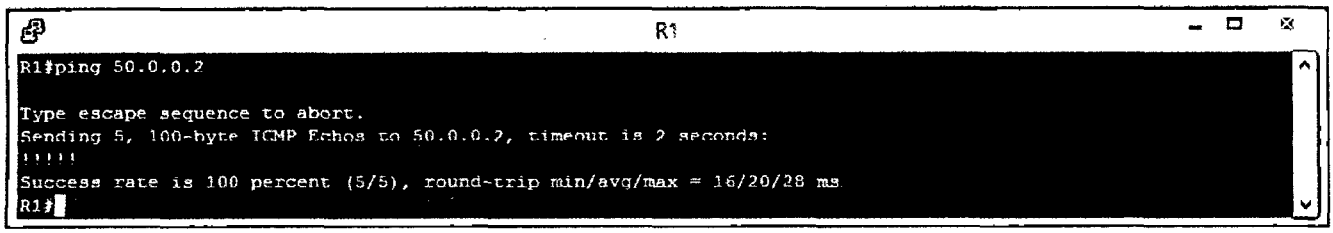


Fig. 4.15.11 Prueba de conectividad a R2.

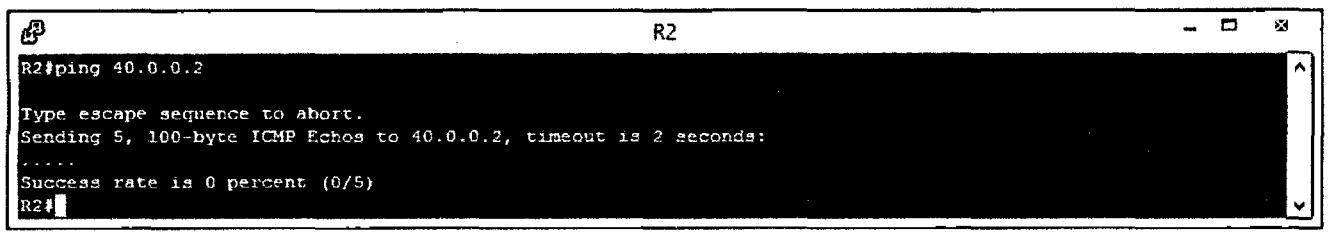


Fig. 4.15.12 Prueba de conectividad a R1.

PASO 2: Acceder al ASDM, mediante un navegador escribiendo la siguiente dirección: https://10.0.0.1

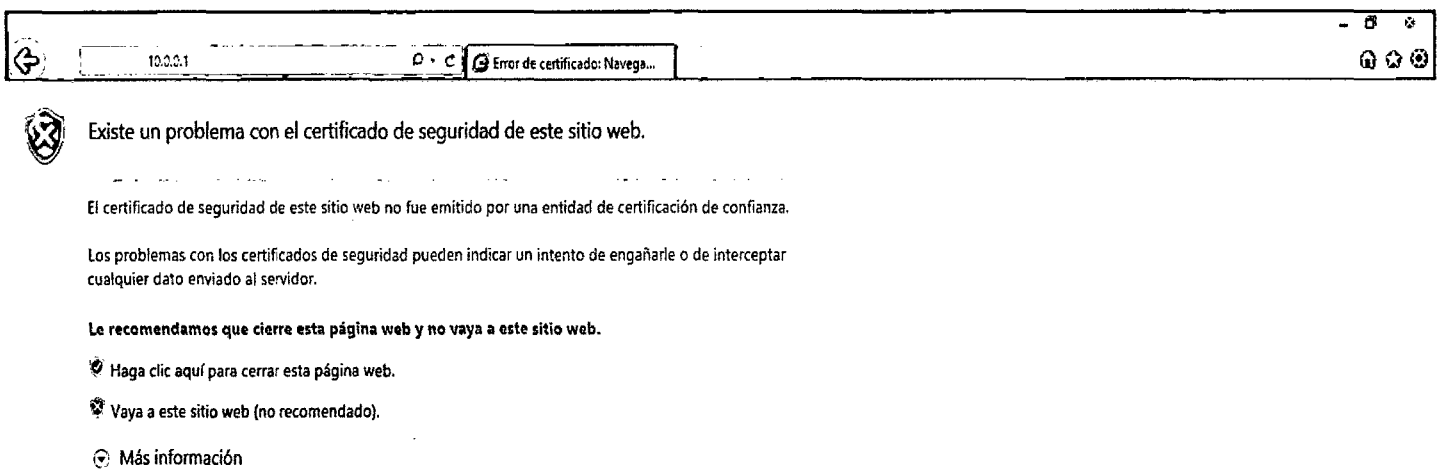


Fig. 4.15.13 Acceder al ASDM.

Luego clic en **Vaya a este sitio web (no recomendado)**

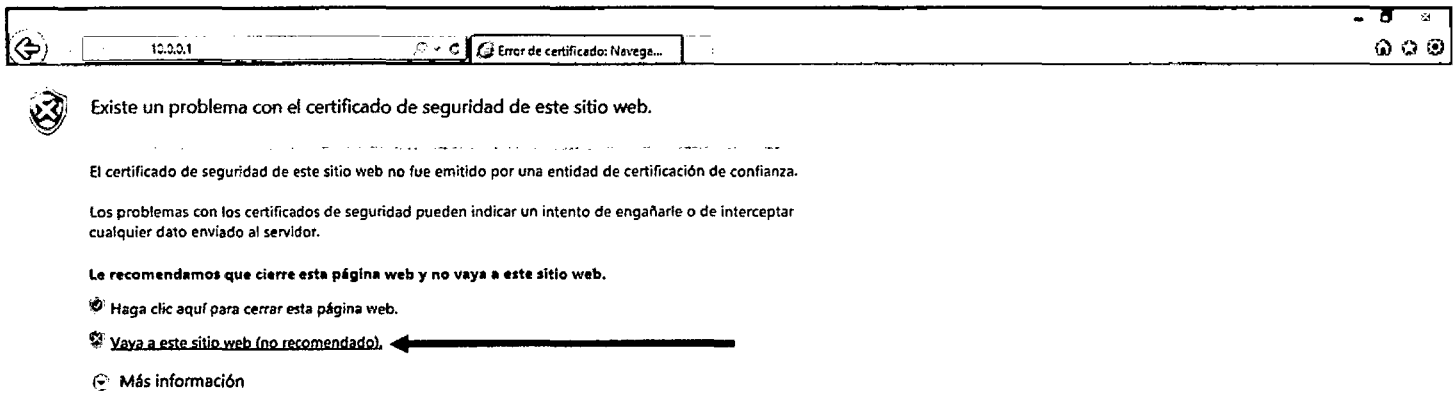


Fig. 4.15.14 Acceder al ASDM.

Escribir usuario y clave:

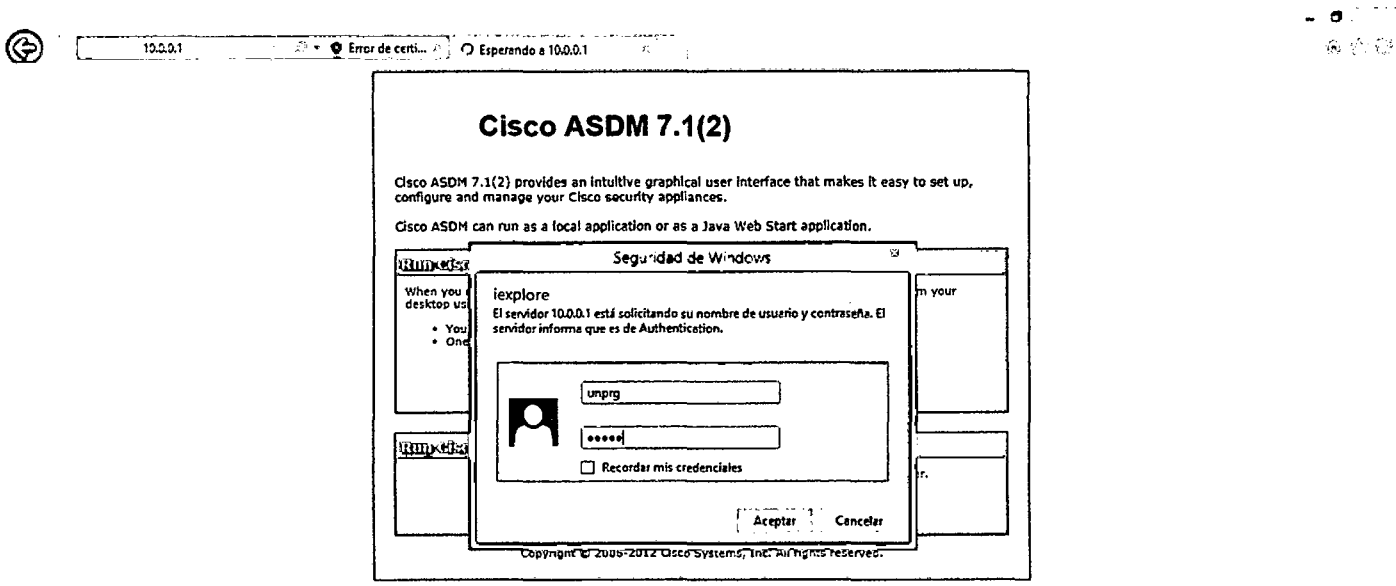


Fig. 4.15.15 Ventana de Seguridad de Windows.

Luego los direccionará a CISCO ASDM-IDM Launcher:

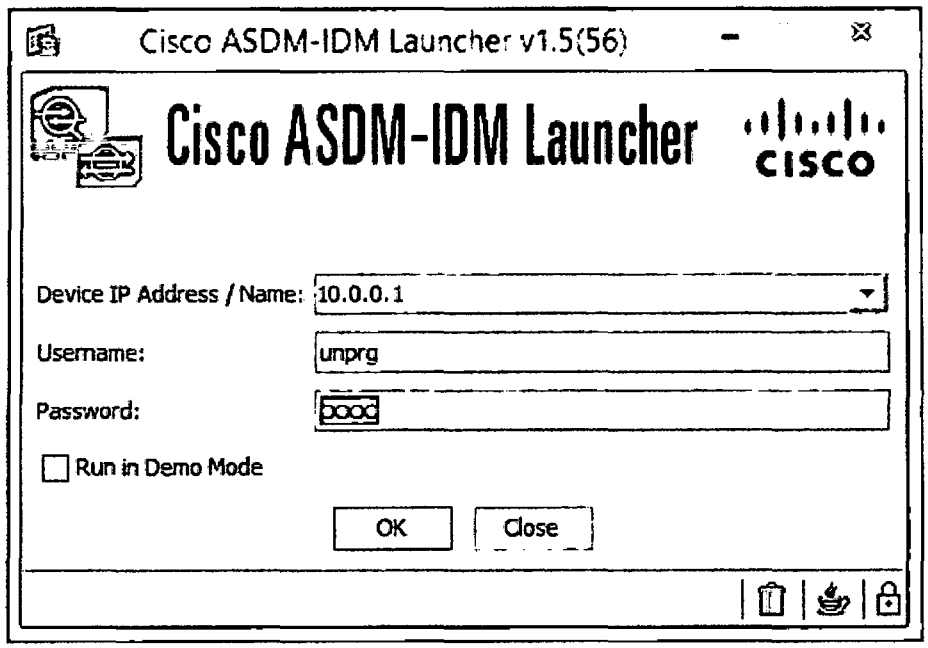


Fig. 4.15.16 Cisco ASDM-IDM Launcher.

Nos mostrara el siguiente cuadro, que seleccionaremos **Continuar:**

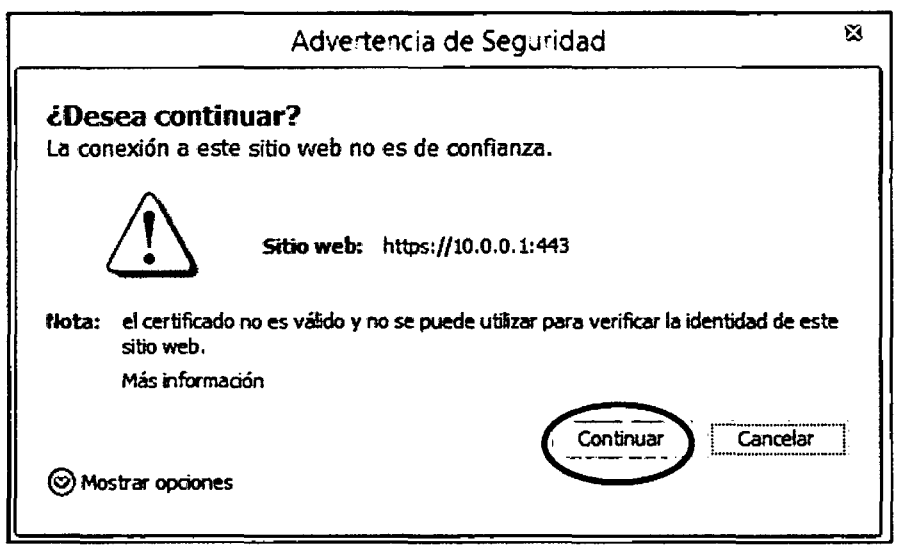


Fig. 4.15.17 Ventana de Advertencia de Seguridad.

Finalmente cargara el ASDM: donde podremos supervisar remotamente el dispositivo ASA y sin necesidad de tener conocimientos amplios en CLI.

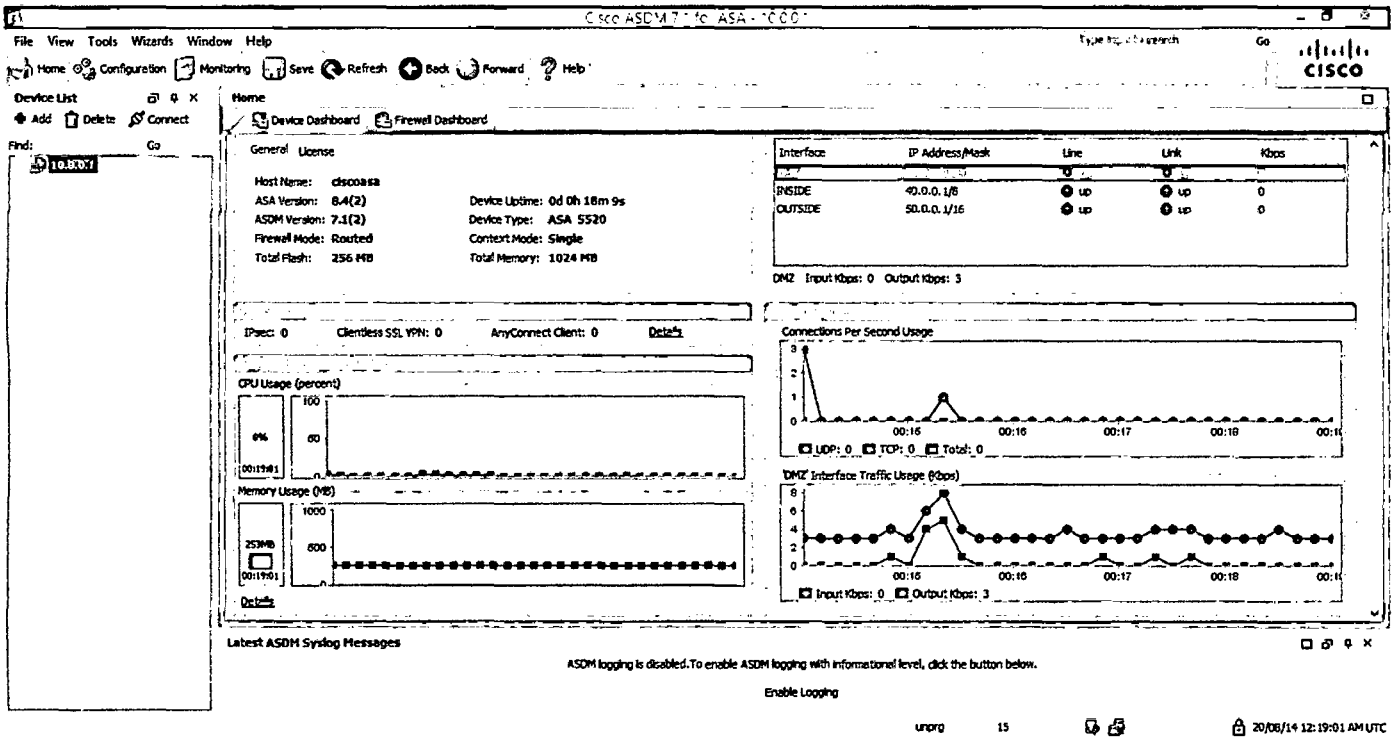


Fig. 4.15.18 Ventana ASDM.

TAREA 7: PROBAR CONECTIVIDAD

PASO 1: Probar conectividad entre los host de la red INSIDE hacia la red OUTSIDE:

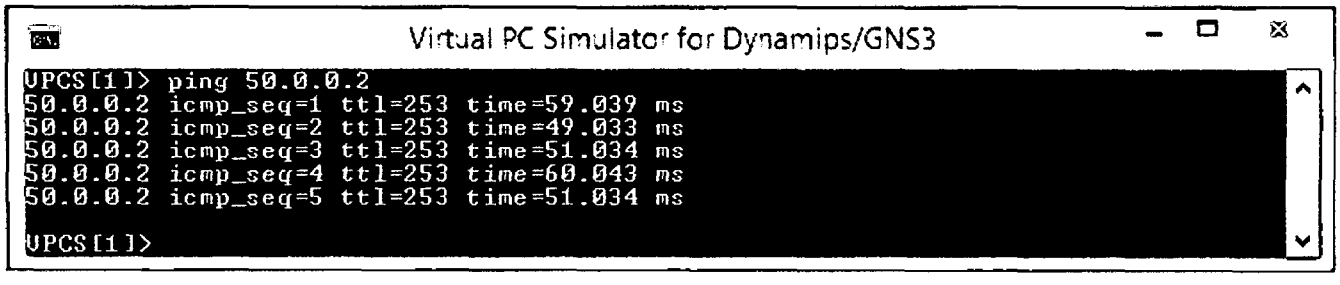


Fig. 4.15.19 Prueba de conectividad de C1 a R2.

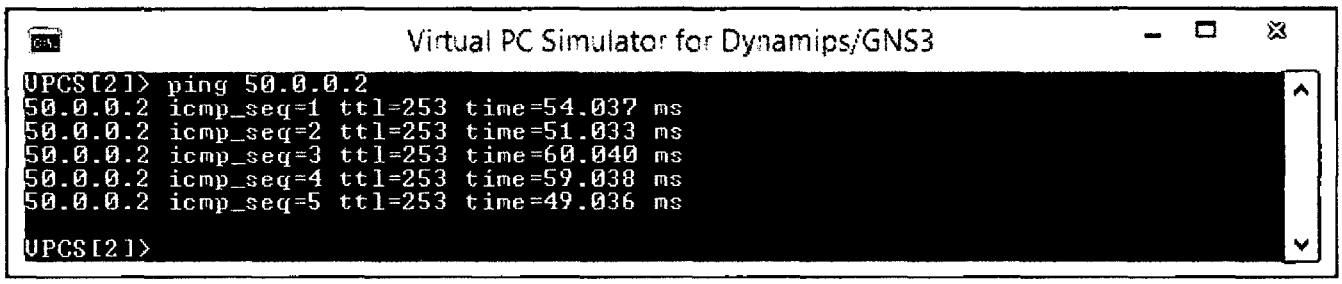


Fig. 4.15.20 Prueba de conectividad de C2 a R2.

PASO 2: Hacer ping desde la red OUTSIDE hacia un host de la red INSIDE, la respuesta debe ser nula:

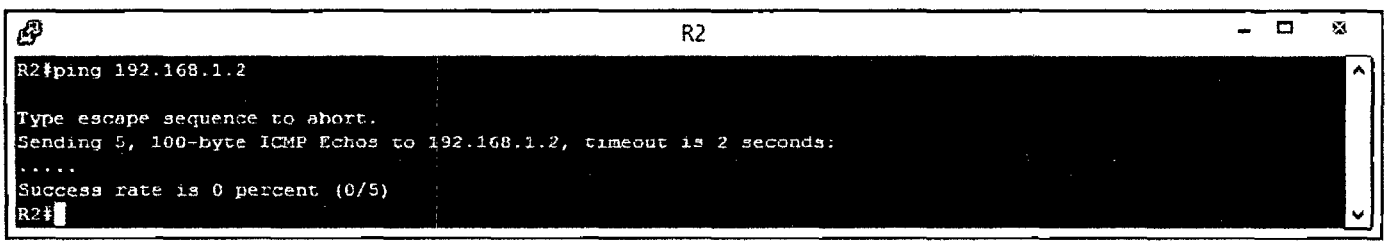


Fig. 4.15.21 Prueba de conectividad de R2 a R3.

LABORATORIO 4.16: REDISTRIBUCION DE PROTOCOLOS

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet.
- Configurar los protocolos: OSPF, EIGRP y RIPV2.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **10.0.0.0/8** para obtener el direccionamiento IP usando VLSM para las interfaces seriales, la dirección **172.16.0.0/30** entre **R1-R2**, **170.20.0.0/30** entre **R4-R5, 170.20.0.4/30** entre **R5-R6** y además teniendo los siguientes requisitos:

LAN R1: 192.168.1.0/24
LAN R2: 192.168.2.0/24
LAN R6: 192.168.3.0/24

DIAGRAMA DE TOPOLOGIA

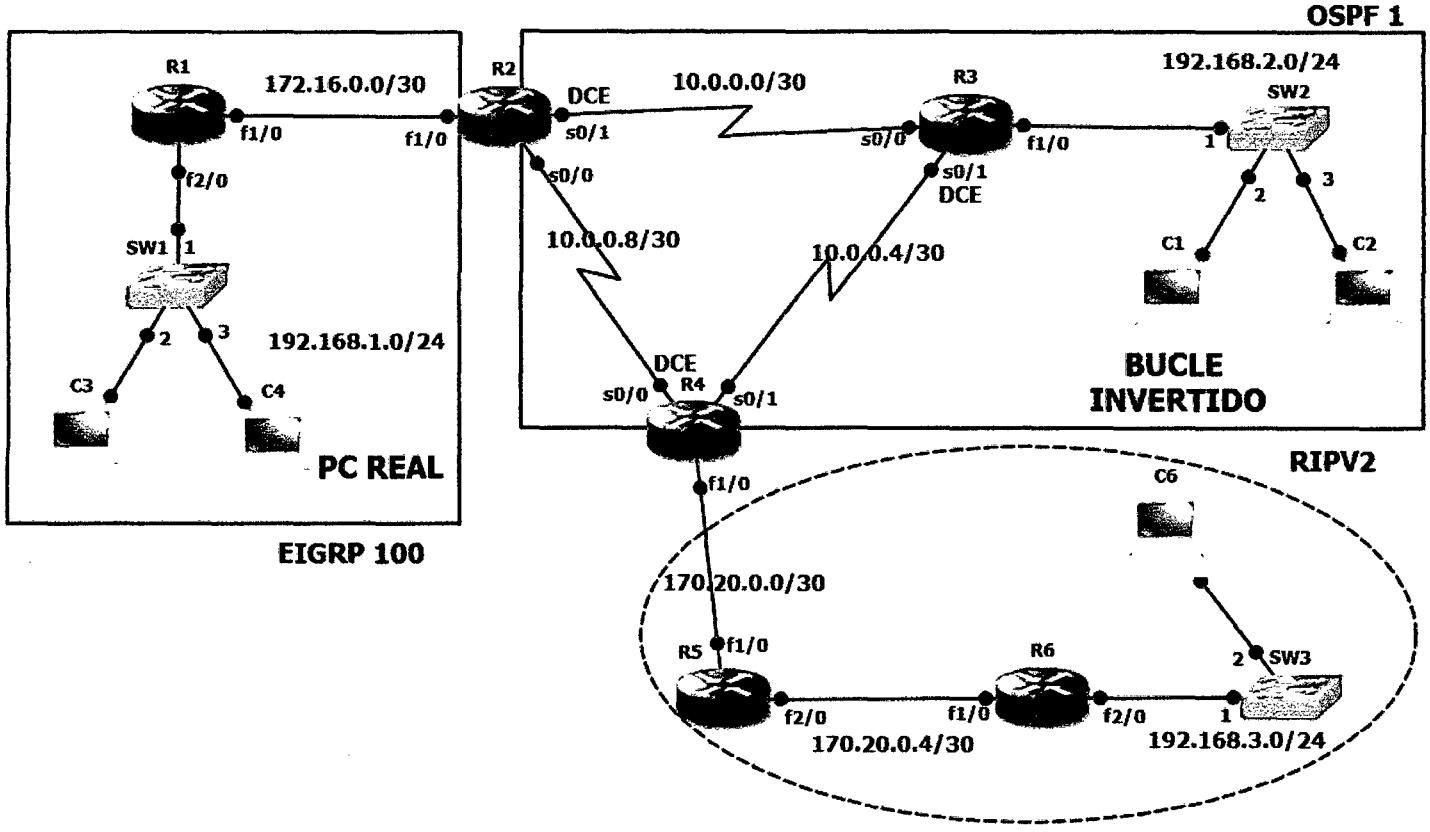


Fig. 4.16.1 Red Virtual en GNS3

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	f1/0	172.16.0.2	255.255.255.252	No aplicable
	f2/0	192.168.1.1	255.255.255.0	No aplicable
R2	s0/0	10.0.0.9	255.255.255.252	No aplicable
	s0/1	10.0.0.1	255.255.255.252	No aplicable
	f1/0	172.16.0.1	255.255.255.0	No aplicable
R3	s0/0	10.0.0.2	255.255.255.252	No aplicable
	s0/1	10.0.0.5	255.255.255.252	No aplicable
	f1/0	192.168.2.1	255.255.255.0	No aplicable
R4	s0/0	10.0.0.10	255.255.255.252	No aplicable
	s0/1	10.0.0.6	255.255.255.252	No aplicable
	f1/0	170.20.0.1	255.255.255.252	No aplicable
R5	f1/0	170.20.0.2	255.255.255.252	No aplicable
	f2/0	170.20.0.5	255.255.255.252	No aplicable
R6	f1/0	170.20.0.6	255.255.255.252	No aplicable
	f2/0	192.168.3.1	255.255.255.0	No aplicable
C1	BUCLE INVERTIDO	192.168.2.2	255.255.255.0	192.168.2.1
C2	VPCS	192.168.2.3	255.255.255.0	192.168.2.1
C3	VPCS	192.168.1.2	255.255.255.0	192.168.1.1
C4	NIC	192.168.1.3	255.255.255.0	192.168.1.1
C6	VPCS	192.168.3.2	255.255.255.0	192.168.3.1

Tabla 4.16.1 Direccionamiento IP para las Redes

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

Montar y conectar la red igual a la del Diagrama de topología.

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

Ingrese al modo privilegiado

Router>enable

Aparece el siguiente prompt

Router#

En el modo exec privilegiado, ingrese al modo de configuración global:

Router# **configure terminal**

PASO 1: Establezca la configuración global del nombre de host.

Ingrese el siguiente comando para configurar el nombre del router:

Router(config)#**hostname XXXXXX** (Escribir nombre deseado)

PASO 2: Desactive la búsqueda DNS.

Router(config)# **no ip-domain lookup**

Si escribes algo que no sea un comando de Cisco IOS o cometes un error, el router asume que ha escrito un nombre de dominio y trata de resolver lo que usted escribe, realizando una búsqueda de DNS.

PASO 3: Configure un mensaje para que se muestre al ingresar al router.

Router(config)#**banner motd %** Solo acceso a personal autorizado **%** (Puede escribir cualquier mensaje)

El símbolo % indica el inicio y final del mensaje.

PASO 4: Configure las contraseñas de consola, enable secret y VTY.

Seguir los siguientes pasos:

Router(config)# **line console 0**

Router(config-line)# **password XXXXX** (Escribir contraseña deseada)

Router(config-line)# **login**

Router(config-line)# **exit**

Router(config)# **enable secret XXXXX** (Escribir contraseña deseada)

Router(config)# **line vty 0 4**

Router(config-line)# **password XXXXX** (Escribir contraseña deseada)

Router(config-line)# **login**

Router(config-line)# **exit**

PASO 5: Sincronice los mensajes no solicitados y el resultado de la depuración con el resultado solicitado y los indicadores para las líneas de consola y de terminal virtual.

Router(config)# **line console 0**

Router(config)# **logging synchronous**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **logging synchronous**

Router(config)# **exit**

PASO 6: Configure un tiempo de espera EXEC de 10 minutos.

Router(config)# **line console 0**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

PASO 7: Guardar la configuración.

Router(config)# **copy running-config startup-config**

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET.

TAREA 4: CONFIGURAR PROTOCOLOS DE ENRUTAMIENTO.

R1:

R1(config)# **router eigrp 100**

R1(config-router)# **network 172.16.0.0**

R1(config-router)# **network 192.168.1.0**

R1(config-router)# **no auto-sumary**

R1(config-router)# **exit**

R2:

R2(config)# **router ospf 1**

R2(config-router)# **network 10.0.0.0 0.0.0.3 area 0**

R2(config-router)# **network 10.0.0.8 0.0.0.3 area 0**

R2(config-router)# **exit**

R2(config-)# **router eigrp 100**

R2(config-router)# **network 172.16.0.0**

R3:

R3(config)# **router ospf 1**

R3(config-router)# **network 10.0.0.0 0.0.0.3 area 0**

R3(config-router)# **network 10.0.0.4 0.0.0.3 area 0**

R3(config-router)# **network 192.168.2.0 0.0.0.255 area 0**

R3(config-router)# **exit**

R4:

R4(config)# **router ospf 1**

R4(config-router)# **network 10.0.0.4 0.0.0.3 area 0**

R4(config-router)# **network 10.0.0.8 0.0.0.3 area 0**

R4(config-router)# **exit**

R4(config)# **router rip**

R4(config-router)# **version 2**

R4(config-router)# **network 170.20.0.0**

R4(config-router)# **no auto-sumary**

R4(config-router)# **exit**

R5:

R5(config)# **router rip**

R5(config)# **version 2**

R5(config-router)# **network 170.20.0.0**

R5(config-router)# **network 170.20.0.4**

R5(config-router)# **no auto-sumary**

R5(config-router)# **exit**

R6:

R6(config)# **router rip**

R6(config)# **version 2**

R6(config-router)# **network 170.20.0.4**

R6(config-router)# **network 192.168.3.0**

R6(config-router)# **no auto-sumary**

R6(config-router)# **exit**

TAREA 5: CONFIGURAR PROTOCOLOS DE REDISTRIBUCION.

Se deben configurar los Routers R2 y R4 ya que harán la redistribución de protocolos.

R2:

R2(config)# **router eigrp 100**

R2(config-router)# **redistribute ospf 1 metric 1000 100 255 1 1500**

R2(config-router)# **exit**

R2(config)# **router ospf 1**

R2(config-router)# **redistribute eigrp 100 subnets**

R2(config-router)# **exit**

R4:

R4(config)# **router ospf 1**

R4(config-router)# **redistribute rip subnets**

R4(config-router)# **exit**

R4(config)# **router rip**

R4(config-router)# **version 2**

R4(config-router)# **redistribute ospf 1 metric 1**

R4(config-router)# **exit**

TAREA 6: CONFIGURAR LOS EQUIPOS DE HOST.

VPCS

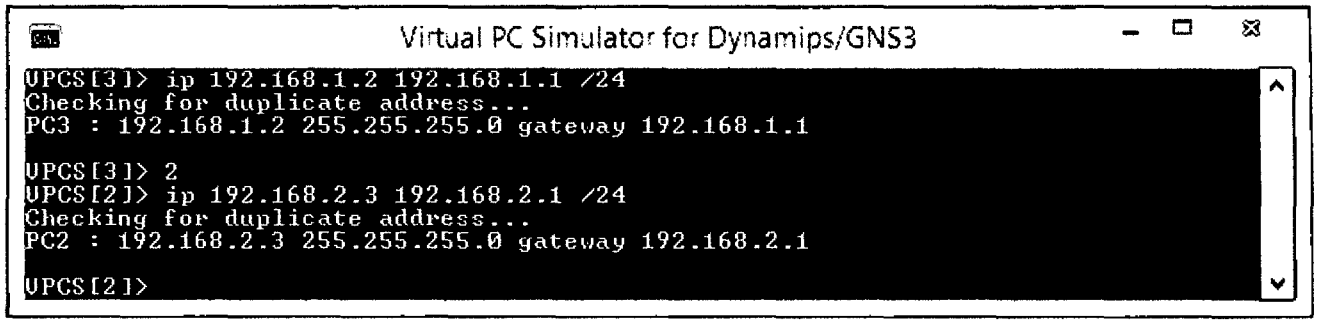


Fig. 4.16.2 Configuración de IP para VPCS.

BUCLE INVERTIDO

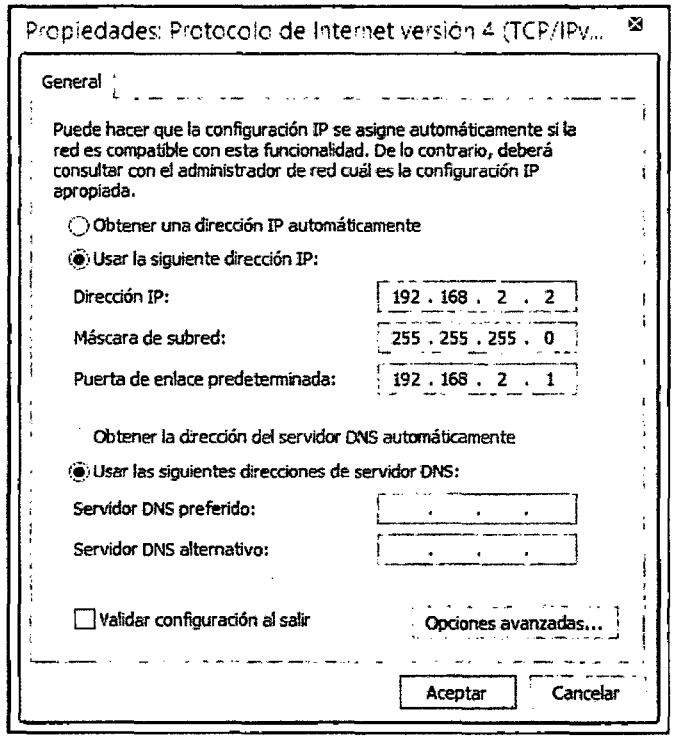


Fig. 4.16.3 Configuración de IP para BUCLE INVERTIDO.

NOTA: Configurar los demás host.

TAREA 7: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

PASO 1: Verificar configuraciones.

R4#show ip route

Muestra el contenido de la tabla de enrutamiento IP.

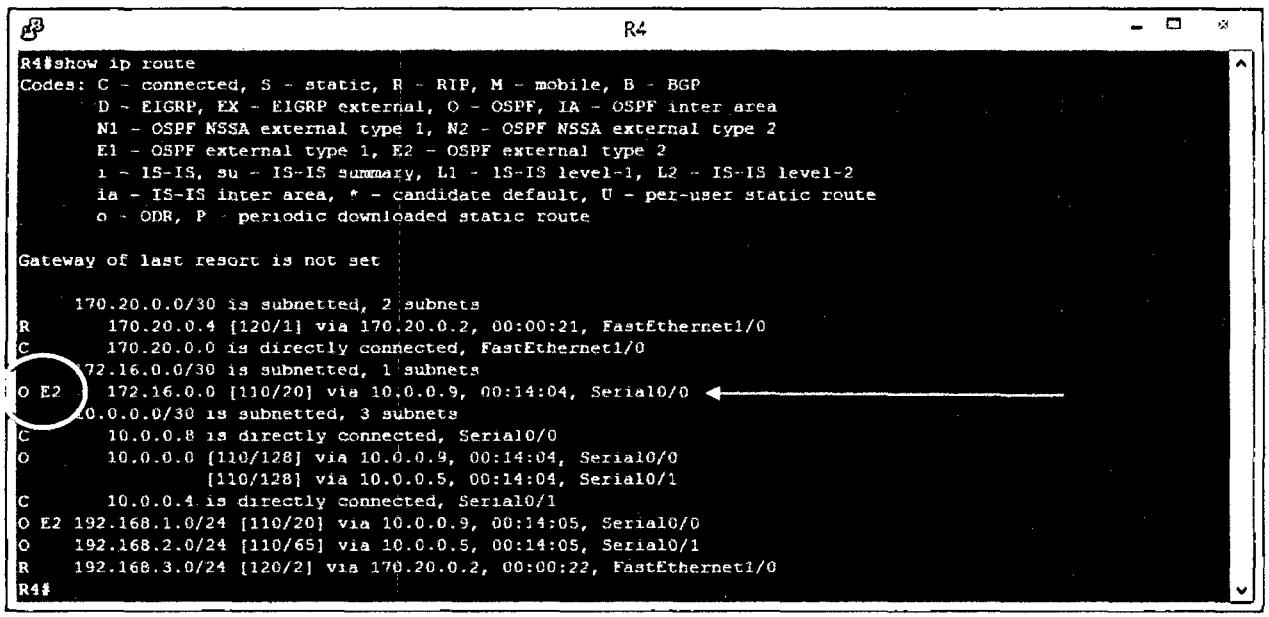


Fig. 4.16.4 Tabla de enrutamiento de R4.

Se muestra dos rutas con la etiqueta de E2, las cuales son rutas importas por otros protocolos; en OSPF la ruta de tipo E2 es por defecto, la cual se puede cambiar también a una de tipo E1.

Ruta externa tipo 1 (E1): las métricas son sumadas al costo de enlace interno

Ruta externa tipo 2 (E2): No añaden ningún costo interno a la métrica.

R4#show ip ospf border-routers

Nos muestra cuales son los routers ASBR (Router de sistema autónomo)

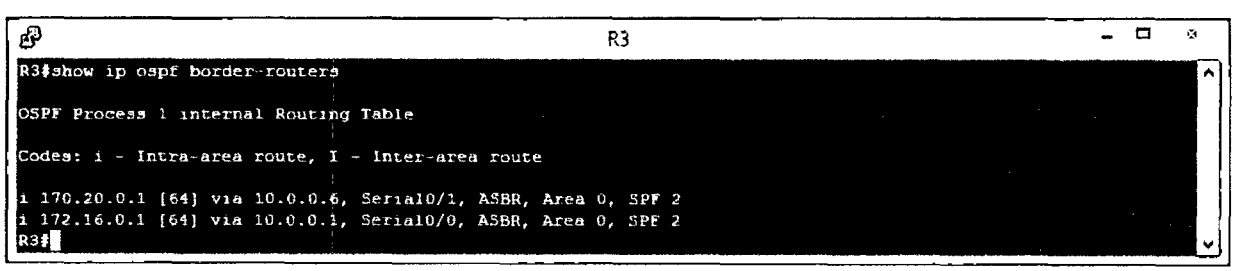


Fig. 4.16.5 Tabla ip ospf border-routers de R3.

R5#show ip route

```
R5
R5#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     170.20.0.0/30 is subnetted, 2 subnets
C       170.20.0.4 is directly connected, FastEthernet2/0
C       170.20.0.0 is directly connected, FastEthernet1/0
     172.16.0.0/30 is subnetted, 1 subnets
R    172.16.0.0 [120/1] via 170.20.0.1, 00:00:21, FastEthernet1/0
     10.0.0.0/30 is subnetted, 3 subnets
R       10.0.0.8 [120/1] via 170.20.0.1, 00:00:21, FastEthernet1/0
R       10.0.0.0 [120/1] via 170.20.0.1, 00:00:21, FastEthernet1/0
R       10.0.0.4 [120/1] via 170.20.0.1, 00:00:21, FastEthernet1/0
R    192.168.1.0/24 [120/1] via 170.20.0.1, 00:00:22, FastEthernet1/0
R    192.168.2.0/24 [120/1] via 170.20.0.1, 00:00:22, FastEthernet1/0
R    192.168.3.0/24 [120/1] via 170.20.0.6, 00:00:18, FastEthernet2/0
R5#
```

Fig. 4.16.6 Tabla de enrutamiento de R5.

Observamos que sus rutas están enunciadas como si fueran RIPv2, debido a que fueron modificadas por R4, el cual se encarga de hacer la redistribución de protocolos.

R1#show ip route

```
R1
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     170.20.0.0/30 is subnetted, 2 subnets
D EX    170.20.0.4 [170/2988160] via 172.16.0.1, 01:20:15, FastEthernet1/0
D EX    170.20.0.0 [170/2988160] via 172.16.0.1, 01:20:15, FastEthernet1/0
     172.16.0.0/30 is subnetted, 1 subnets
C       172.16.0.0 is directly connected, FastEthernet1/0
     10.0.0.0/30 is subnetted, 3 subnets
D EX    10.0.0.8 [170/2588160] via 172.16.0.1, 01:20:28, FastEthernet1/0
D EX    10.0.0.0 [170/2588160] via 172.16.0.1, 01:20:28, FastEthernet1/0
D EX    10.0.0.4 [170/2588160] via 172.16.0.1, 01:20:16, FastEthernet1/0
C    192.168.1.0/24 is directly connected, FastEthernet2/0
D EX 192.168.2.0/24 [170/2588160] via 172.16.0.1, 01:20:16, FastEthernet1/0
D EX 192.168.3.0/24 [170/2588160] via 172.16.0.1, 01:20:16, FastEthernet1/0
R1#
```

Fig. 4.16.7 Tabla de enrutamiento de R1.

De igual manera podemos observar en R1 que las rutas están enunciadas como EIGRP de tipo EX (external)

PASO 2: Utilice el comando ping para probar la conectividad entre los routers que no están directamente conectados y también la conectividad entre host.

PING ENTRE ROUTERS

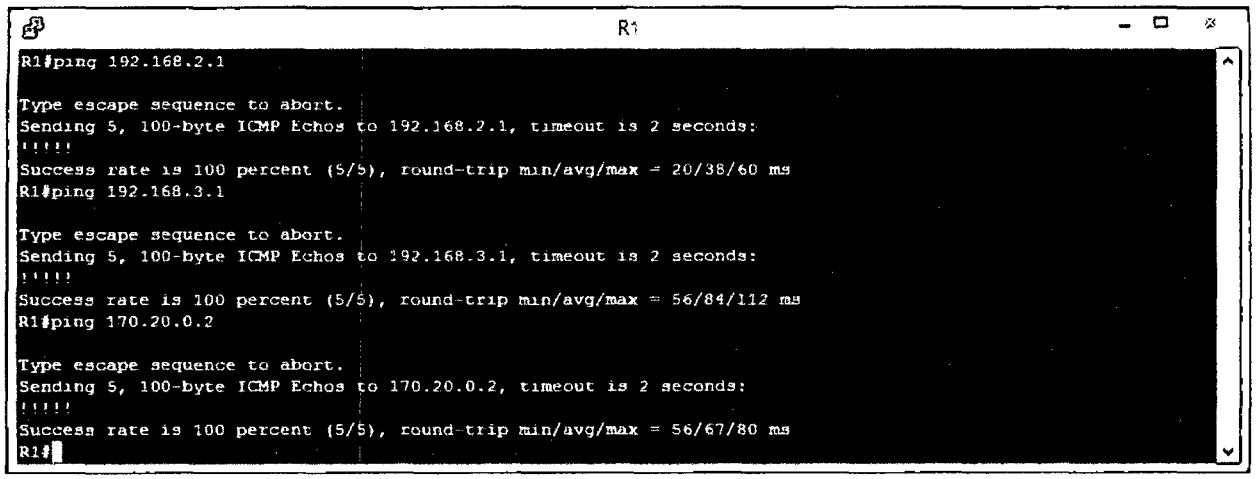


Fig. 4.16.8 Prueba de conectividad entre routers.

PING ENTRE HOST

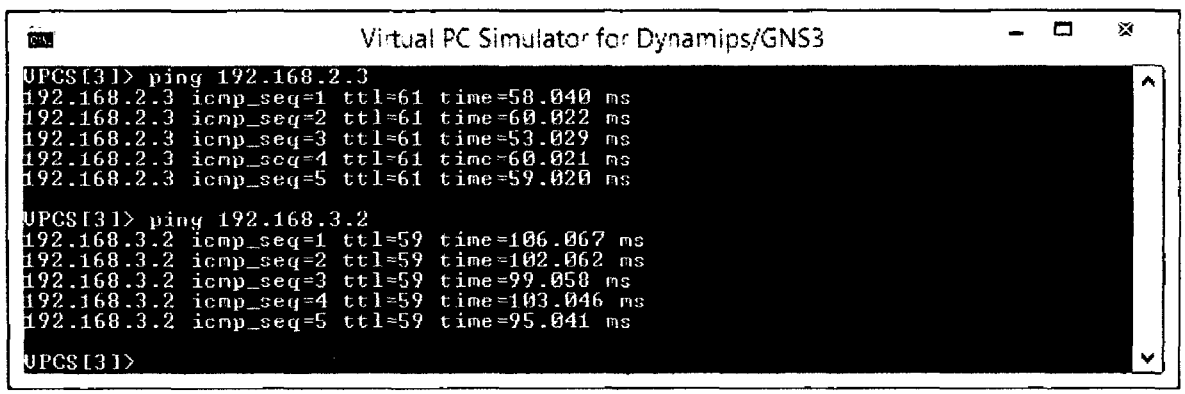


Fig. 4.16.9 Prueba de conectividad entre host.

NOTA: Realizar las pruebas faltantes.

TAREA 7: ANALISIS DEL TRAFICO DE PAQUETES

PASO 1: Medición de la Latencia

Para la medición de la latencia se realizó 10 muestras sucesivas de 100 ping desde el C2 (Bucle invertido) hacia la PC REAL considerando un tamaño de trama de 64, 512 y 1518 bytes como se especifica en el RFC 2544.

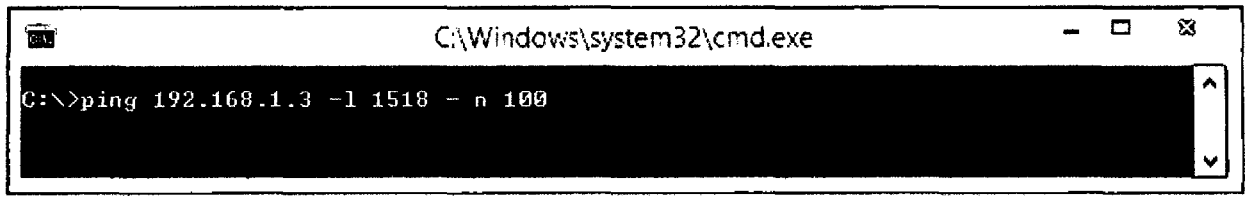


Fig. 4.16.10 Prueba de conectividad entre host.

En la Figura 4.16.10 se puede observar el envío de 100 ping con una trama de 1518 hacia la dirección 192.168.1.3

En las Tablas posteriores se detallan los valores de la Latencia que se ha obtenido una vez realizadas todas las muestras.

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	N° 1	**N° 2**	**N° 3**	**N° 4**	**N° 5**	**N° 6**	**N° 7**	**N° 8**	**N° 9**	**N° 10**	**Promedio**
Tiempo Mínimo (ms)	**80**	**85**	**79**	**82**	**89**	**80**	**79**	**82**	**79**	**83**	**81.8**
Tiempo Máximo (ms)	**111**	**93**	**97**	**98**	**94**	**98**	**95**	**89**	**97**	**99**	**97.1**
Tiempo Promedio (ms)	**87**	**87**	**90**	**85**	**91**	**87**	**88**	**85**	**89**	**87**	**87.6**

Tabla 4.16.2 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	512										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	88	65	87	85	84	85	85	86	83	82	83
Tiempo Máximo (ms)	119	98	95	96	95	95	98	117	96	100	100.9
Tiempo Promedio (ms)	92	87	90	89	89	88	89	90	90	88	89.2

Tabla 4.16.3 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1518										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	83	88	87	88	81	88	84	83	84	85	85.1
Tiempo Máximo (ms)	99	99	100	96	98	98	99	100	98	100	105
Tiempo Promedio (ms)	87	93	89	91	94	91	92	92	90	88	91.6

Tabla 4.16.4 Datos obtenidos para una trama de 1518 bytes.

LATENCIA			
Tamaño de Trama (bytes)	64	512	1518
Tiempo Mínimo (ms)	81.8	83	85.1
Tiempo Máximo (ms)	97.1	100.9	105
Tiempo Promedio (ms)	87.6	89.2	91.6

Tabla 4.16.5 Comparación de datos obtenidos de las diferentes tramas.

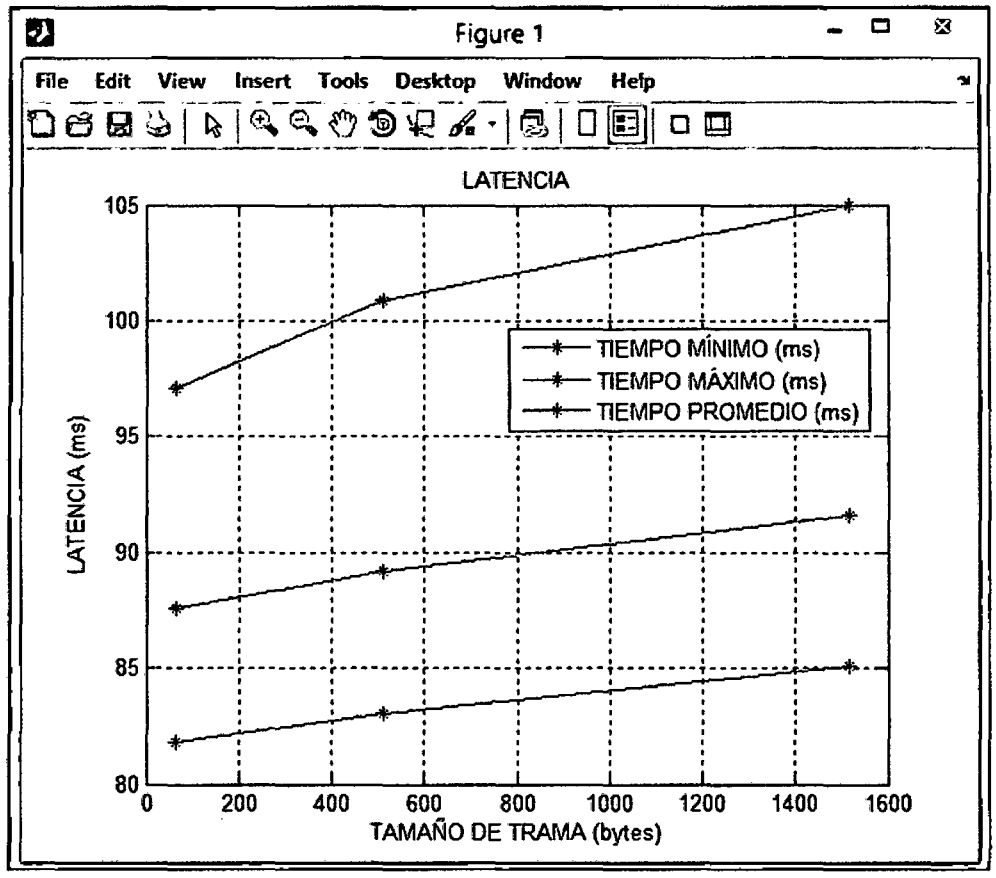


Fig. 4.16.11 Datos representados gráficamente de la variación de la latencia.

De acuerdo con los datos obtenidos, se puede observar claramente que los valores mínimo (color azul), máximo (color rojo) y promedio (color verde) de la latencia de la red se incrementan conforme se envía una trama de longitud mayor, en este caso con la trama de 1518 bytes se obtiene una latencia promedio de 91.6 ms a diferencia de una trama de 64 bytes con 87.6 ms.

PASO 2: Medición del Throughput

Para la medición del Throughput y Jitter se envió una cantidad de tramas a velocidades diferentes durante 20 segundos, hasta encontrar la máxima cantidad de tramas recibidas sin que se produzcan perdidas de las mismas en el router y PC REAL. Como se utilizó Jperf el cliente será el encargado de enviar los paquetes y el servidor los recibirá, indicando la cantidad de paquetes que llegaron correctamente considerando un tamaño del paquete UDP de 750, 1125, 1500 y 1470 (default) bytes, tal como se especifica en el RFC 768.

Configuración del Jperf como servidor con UDP Packet Size de 1125 Bytes.

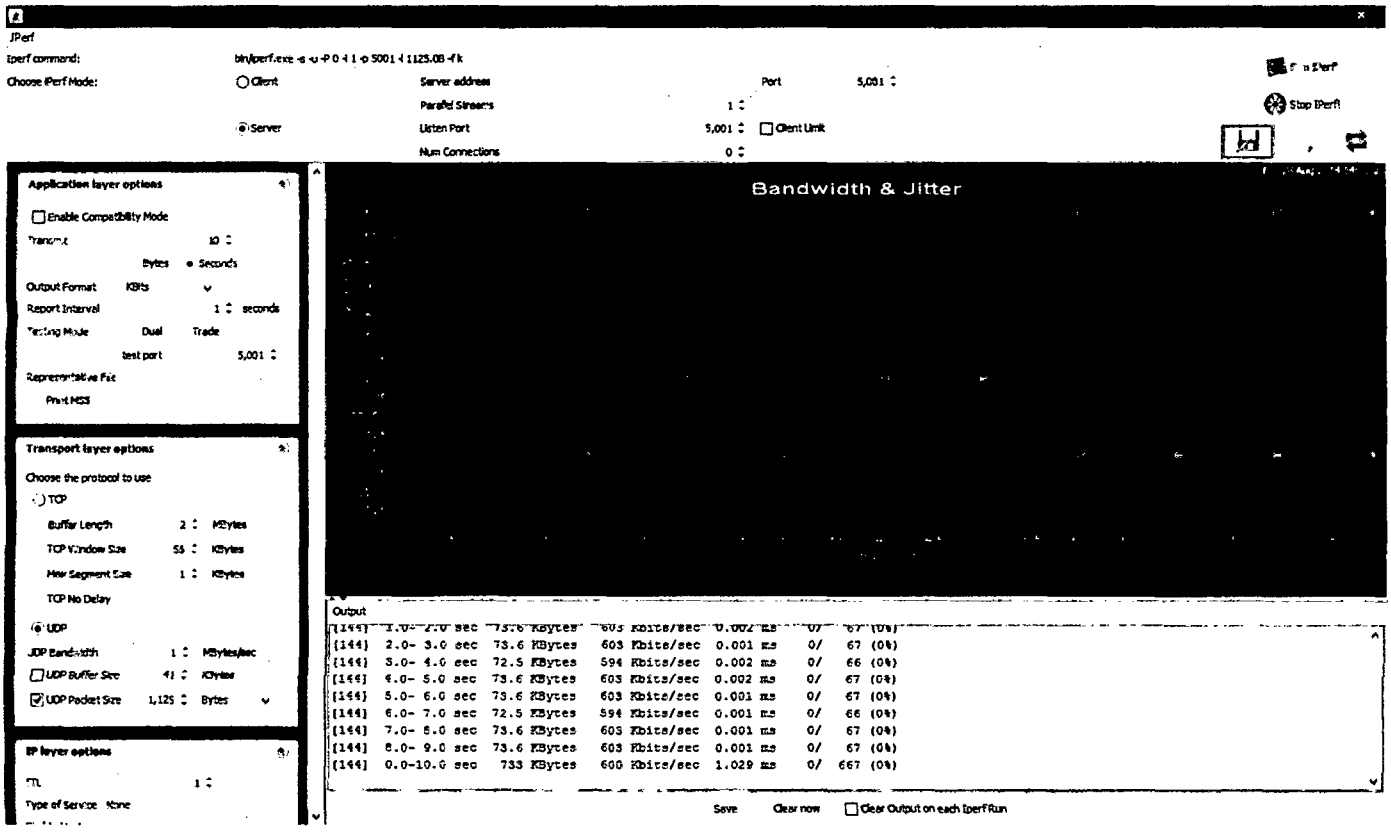


Fig. 4.16.12 Gráfica de Bandwidth y Jitter.

```
bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -l 1125.0B -f k
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1125 byte datagrams
UDP buffer size: 64.0 KByte (default)
------------------------------------------------------------
OpenSCManager failed - Acceso denegado. (0x5)
[144] local 192.168.1.3 port 5001 connected with 192.168.2.2 port 62334
[ ID] Interval       Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[144]  0.0- 1.0 sec  73.6 KBytes   603 Kbits/sec  0.001 ms 1546661425/   67 (2.3e+009%)
[144]  1.0- 2.0 sec  73.6 KBytes   603 Kbits/sec  0.002 ms    0/   67 (0%)
[144]  2.0- 3.0 sec  73.6 KBytes   603 Kbits/sec  0.001 ms    0/   67 (0%)
[144]  3.0- 4.0 sec  72.5 KBytes   594 Kbits/sec  0.002 ms    0/   66 (0%)
[144]  4.0- 5.0 sec  73.6 KBytes   603 Kbits/sec  0.002 ms    0/   67 (0%)
[144]  5.0- 6.0 sec  73.6 KBytes   603 Kbits/sec  0.001 ms    0/   67 (0%)
[144]  6.0- 7.0 sec  72.5 KBytes   594 Kbits/sec  0.001 ms    0/   66 (0%)
[144]  7.0- 8.0 sec  73.6 KBytes   603 Kbits/sec  0.001 ms    0/   67 (0%)
[144]  8.0- 9.0 sec  73.6 KBytes   603 Kbits/sec  0.001 ms    0/   67 (0%)
[144]  0.0-10.0 sec   733 KBytes   600 Kbits/sec  1.029 ms    0/  667 (0%)
```

Fig. 4.16.13 Resultados al medir como servidor.

Configuración del Jperf como cliente con UDP Bandwidth de 600 Kbps y UDP Packet Size de 1125 Bytes.

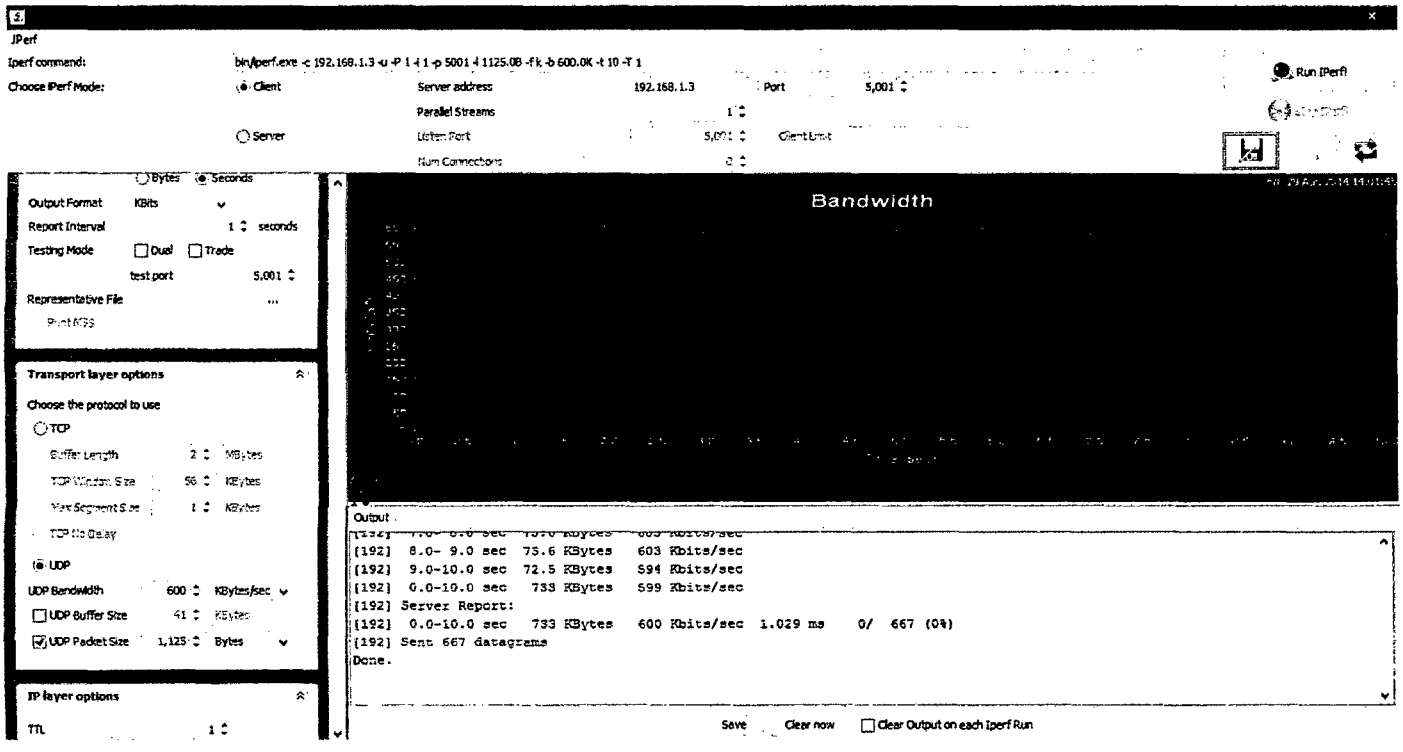


Fig. 4.16.14 Resultados del Jperf como Cliente al medir Throughput.

En las siguientes Tablas se detalla los valores del Throughput obtenidos una vez realizada todas las muestras.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**0.6**	**0.6**	**0.6**
Velocidad de Rx (Mbps)	**0.6**	**0.6**	**0.6**
Tramas Transmitidas	**1000**	**667**	**501**
Tramas Recibidas	**1000**	**667**	**501**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**100**	**66.7**	**50.1**

Tabla 4.16.6 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**0.4**	**0.6**	**1**
Velocidad de Rx (Mbps)	**0.4**	**0.6**	**1**
Tramas Transmitidas	**341**	**511**	**851**
Tramas Recibidas	**341**	**511**	**851**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**34.1**	**51.1**	**85.1**

Tabla 4.16.7 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

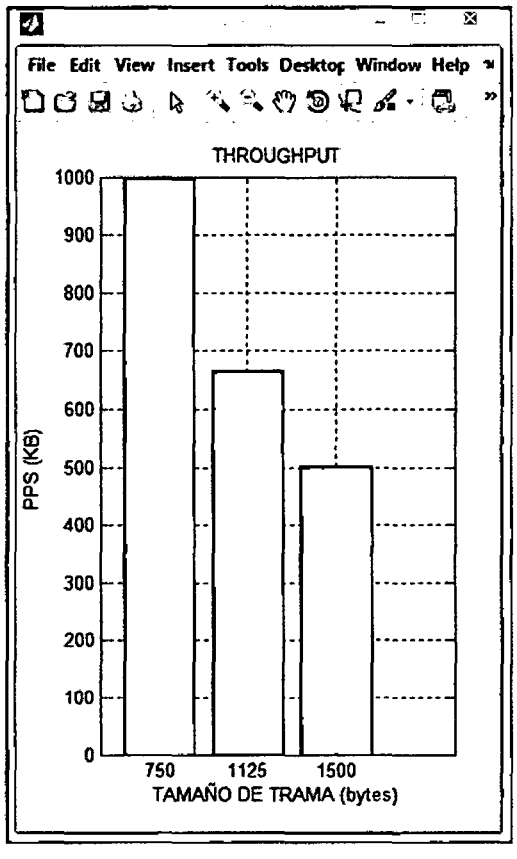


Fig. 4.16.15 PPS vs. Tamaño de Trama.

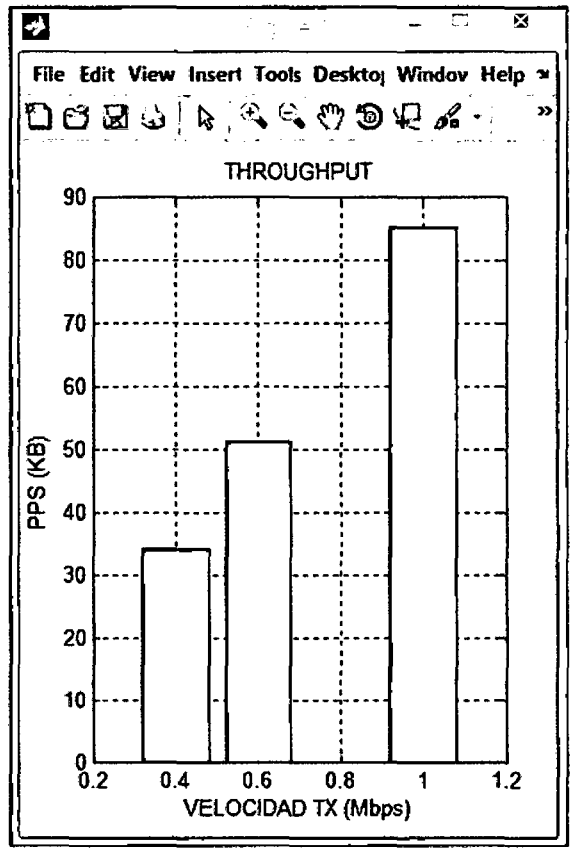


Fig. 4.16.16 PPS vs. Velocidad Tx.

En la figura 4.16.15, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 750 bytes, 1125 bytes y 1500 bytes los cuales han utilizado una velocidad de Tx constante de 0.6 Mbps, en la gráfica se puede observar claramente que al enviar una trama de 750 bytes se envía 1000 pps, con una trama de 1125 se envía 667 pps y con una trama de 1500 se envía 501 pps.

Mientras en la figura 4.16.16, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 1470 bytes los cuales han utilizado una velocidad de Tx variada de: 0.4 Mbps, 0.6 Mbps y 1 Mbps, sin que se produzcan perdidas en el envío, como los datos que se muestran en la tabla 4.16.7.

PASO 3: Medición del Jitter

Para la medición se envió datos UDP de longitud variable a velocidades diferentes de Throughput obtenida anteriormente durante 20 segundos. Como se utilizó anteriormente Jperf el cliente será el encargado de enviar los datos y el servidor los recibirá, indicando los valores de Jitter obtenidos durante la transmisión de los datos.

Configuración del Jperf como servidor con UDP Packet Size por defecto.

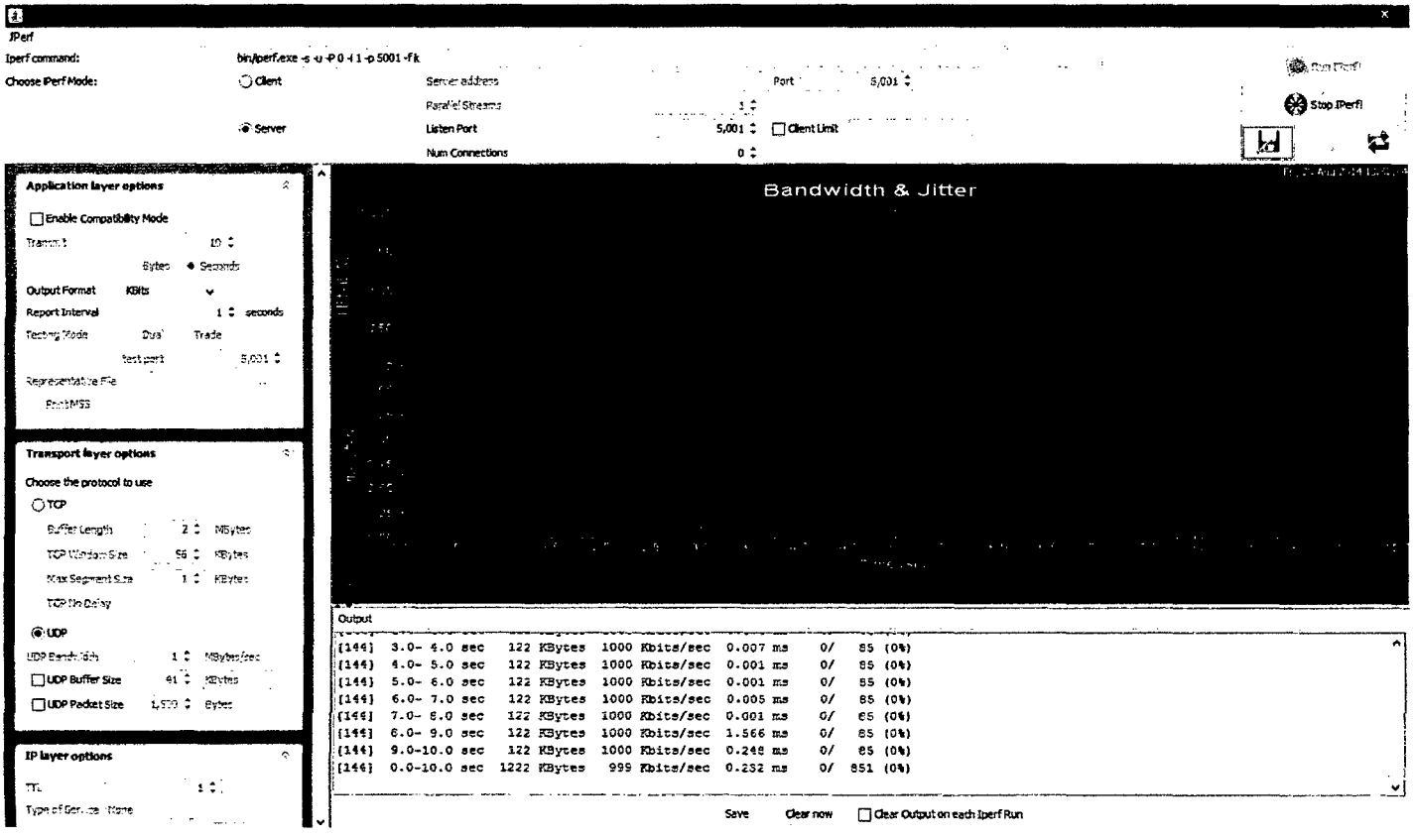


Fig. 4.16.17 Gráfica de Bandwidth y Jitter.

```
bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -f k
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 64.0 KByte (default)
------------------------------------------------------------
OpenSCManager failed - Acceso denegado. (0x5)
[144] local 192.168.1.3 port 5001 connected with 192.168.2.2 port 56137
[ ID] Interval       Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[144]  0.0- 1.0 sec   122 KBytes  1000 Kbits/sec  0.001 ms 1546661425/   85 (1.8e+009%)
[144]  1.0- 2.0 sec   122 KBytes  1000 Kbits/sec  0.008 ms    0/   85 (0%)
[144]  2.0- 3.0 sec   122 KBytes  1000 Kbits/sec  0.076 ms    0/   85 (0%)
[144]  3.0- 4.0 sec   122 KBytes  1000 Kbits/sec  0.007 ms    0/   85 (0%)
[144]  4.0- 5.0 sec   122 KBytes  1000 Kbits/sec  0.001 ms    0/   85 (0%)
[144]  5.0- 6.0 sec   122 KBytes  1000 Kbits/sec  0.001 ms    0/   85 (0%)
[144]  6.0- 7.0 sec   122 KBytes  1000 Kbits/sec  0.005 ms    0/   85 (0%)
[144]  7.0- 8.0 sec   122 KBytes  1000 Kbits/sec  0.001 ms    0/   85 (0%)
[144]  8.0- 9.0 sec   122 KBytes  1000 Kbits/sec  1.566 ms    0/   85 (0%)
[144]  9.0-10.0 sec   122 KBytes  1000 Kbits/sec  0.248 ms    0/   85 (0%)
[144]  0.0-10.0 sec  1222 KBytes   999 Kbits/sec  0.232 ms    0/  851 (0%)
```

Fig. 4.16.18 Resultados al medir como servidor.

En las siguientes Tablas se detalla los valores del Jitter obtenidos una vez realizada todas las muestras.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**0.6**	**0.6**	**0.6**
Velocidad de Rx (Mbps)	**0.6**	**0.6**	**0.6**
Tramas Transmitidas	**1000**	**667**	**501**
Tramas Recibidas	**1000**	**667**	**501**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**0.689**	**1.029**	**1.523**

Tabla 4.16.8 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**0.4**	**0.6**	**1**
Velocidad de Rx (Mbps)	**0.4**	**0.6**	**1**
Tramas Transmitidas	**341**	**511**	**851**
Tramas Recibidas	**341**	**511**	**851**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**0.002**	**0.130**	**0.232**

Tabla 4.16.9 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

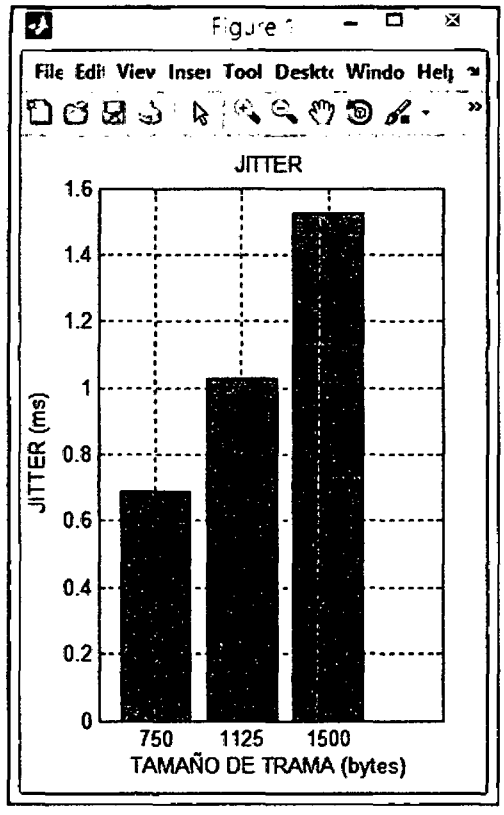


Fig. 4.16.19 Jitter vs. Tamaño de Trama Tx

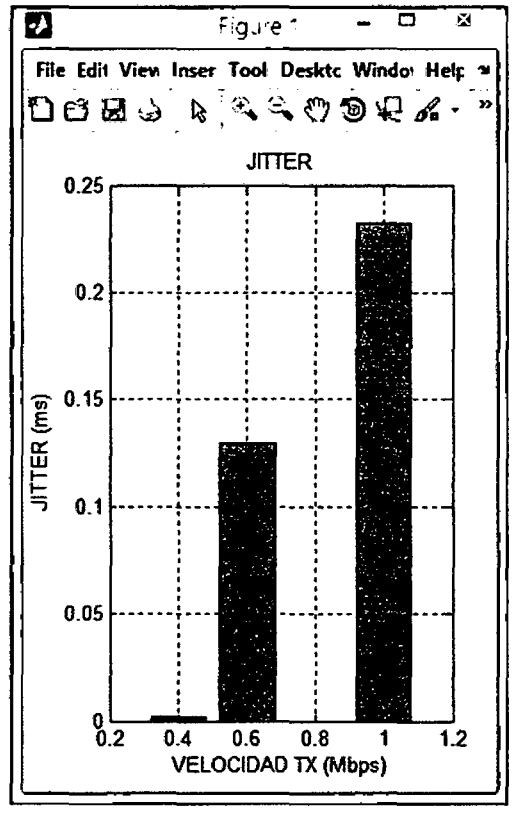


Fig. 4.16.20 Jitter vs. Velocidad

En la figura 4.16.19 se observa los valores del Jitter obtenidos al enviar diferentes tamaños de paquete UDP como 750, 1125 y 1500 bytes utilizando una velocidad de Tx constante de 0.6 Mbps, se puede observar claramente que con una trama de 750 bytes se tiene un Jitter de 0.689 ms a diferencia de la trama de 1500 bytes en la cual se tiene un Jitter de 1.523 ms.

En la figura 4.16.20, se observa los valores del Jitter obtenidos al enviar paquetes UDP de 1470 bytes utilizando una velocidad de Tx que varía de: 0.4 Mbps, 0.6 Mbps y 1 Mbps, sin que se pierdan paquetes en la red.

PASO 4: Captura de tráfico con Wireshark.

Capturar tráfico de paquetes en la interfaz f1/0 de R4.

- Captura de paquetes RIPV2.

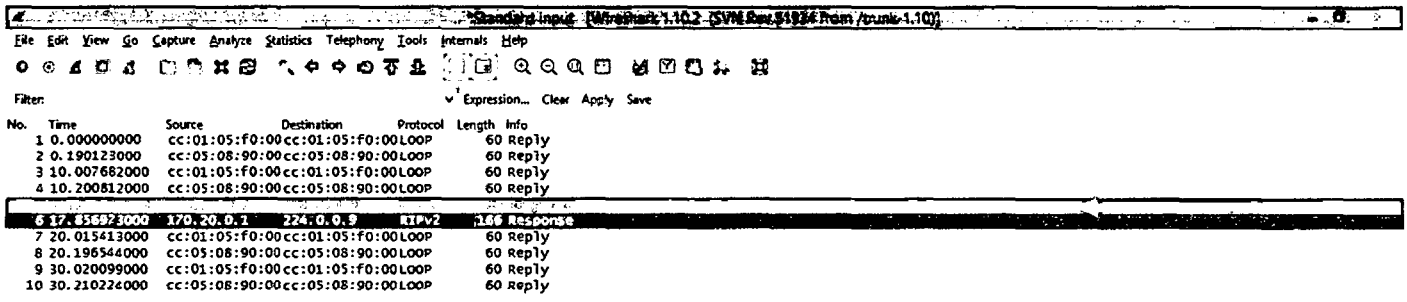


Fig. 4.16.21 Captura de paquete RIPV2 con Wireshark.

- Captura de paquetes ICMP.

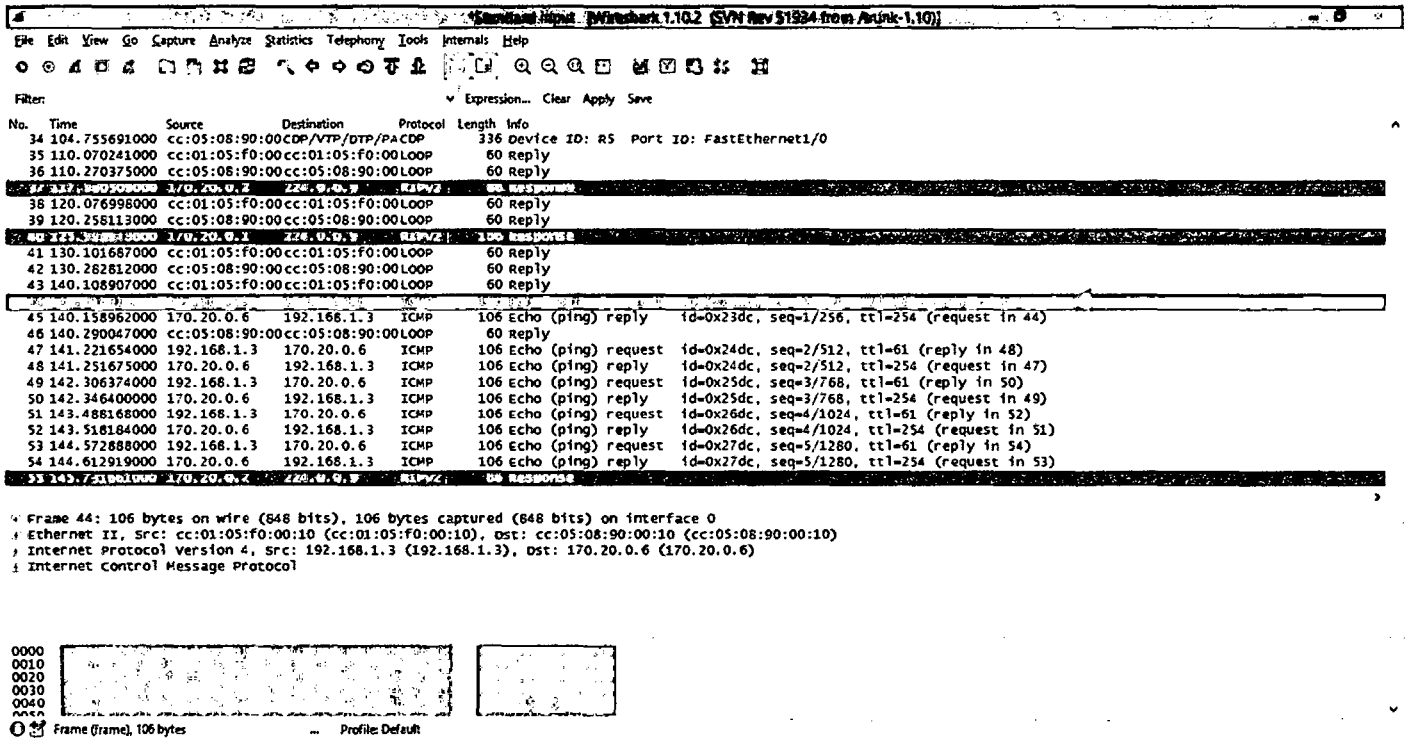


Fig. 4.16.22 Captura de paquete ICMP con Wireshark.

Capturar tráfico de paquetes en la interfaz s0/0 de R4.

- Captura de paquetes HELLO OSPF.

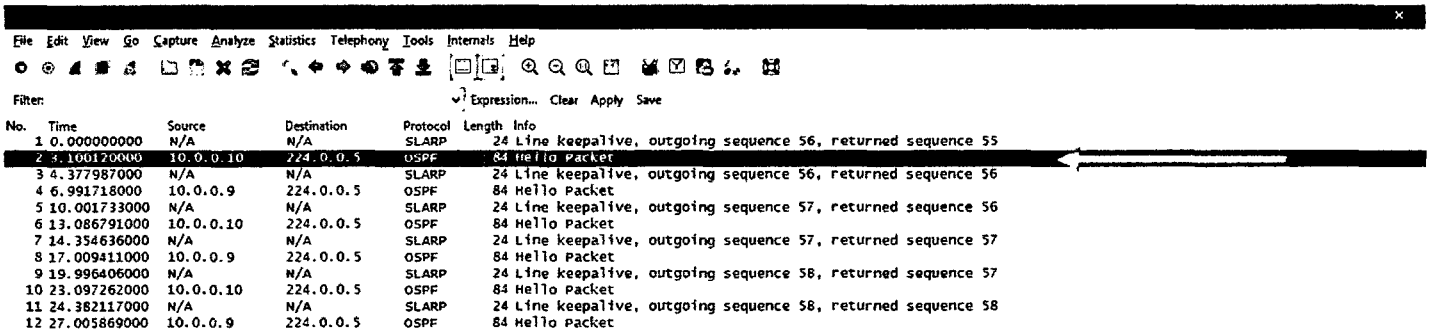


Fig. 4.16.23 Captura de paquete HELLO OSPF con Wireshark.

Capturar tráfico de paquetes en la interfaz f1/0 de R2.

- Captura de paquetes HELLO OSPF.

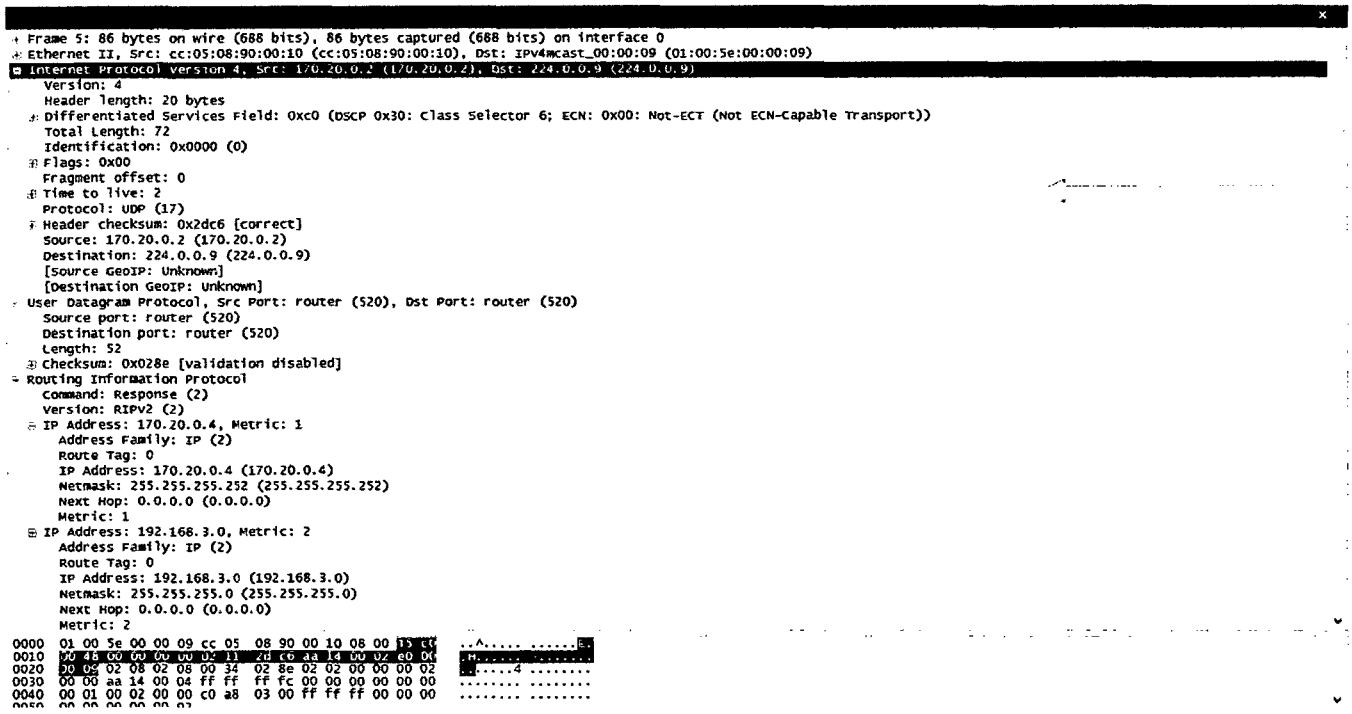


Fig. 4.16.24 Información detallada del paquete HELLO OSPF.

Capturar tráfico de paquetes en la interfaz s0/0 de R3.

- Captura de paquetes Telnet.

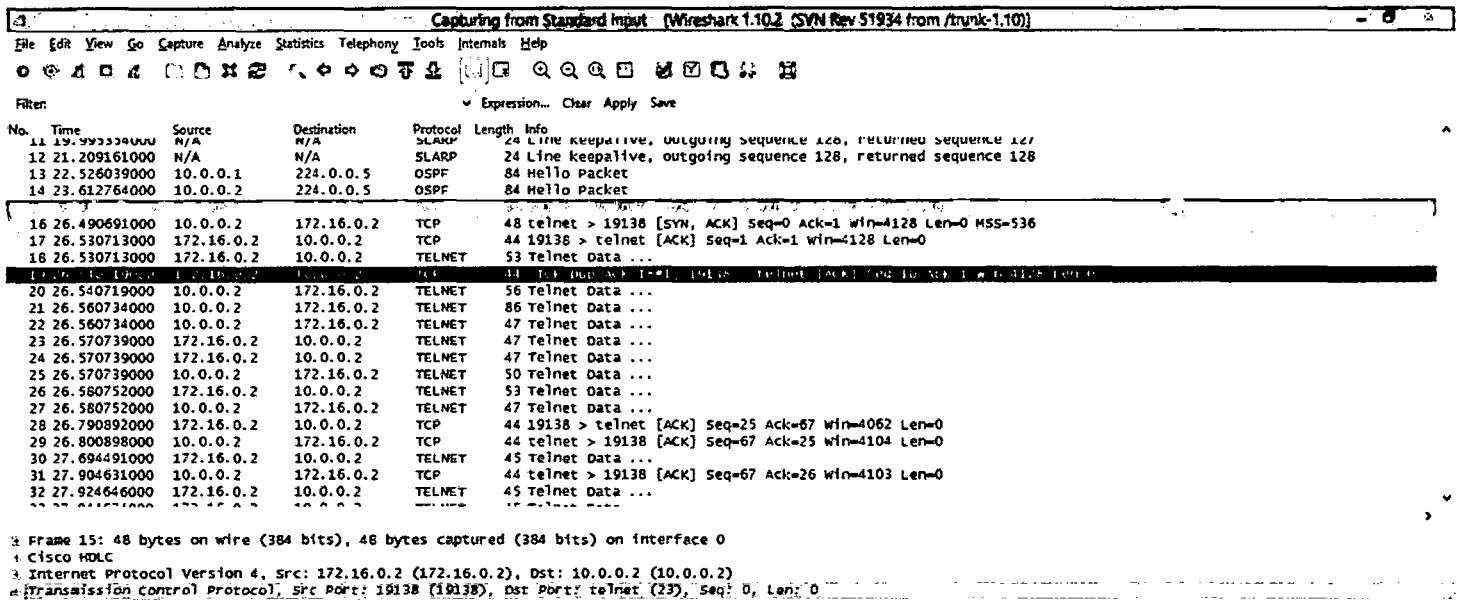


Fig. 4.16.25 Captura de paquete telnet con Wireshark.

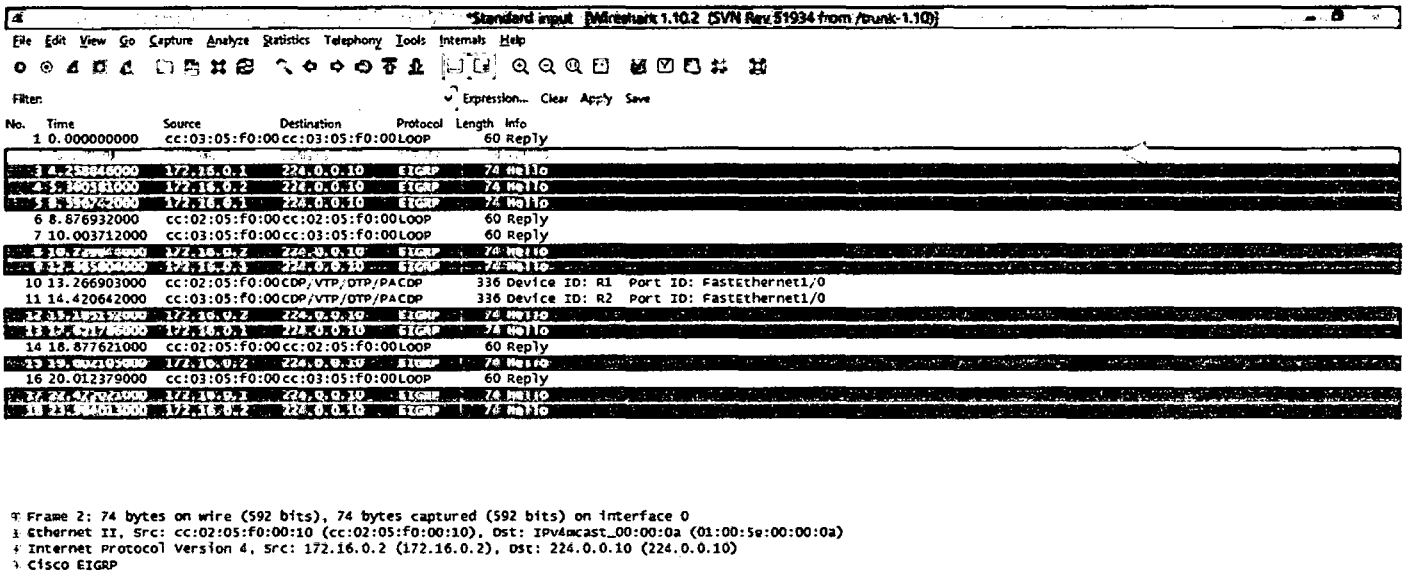


Fig. 4.16.26 Captura de paquete HELLO EIGRP con Wireshark.

LABORATORIO 4.17: IPV6

REVISIÓN TEÓRICA: Para la realización de esta práctica se deberá revisar conceptos de IPV6.

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet.
- Configurar IPV6 Tunneling.
- Configurar IPV6 RIPNG.
- Configurar EIGRP.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **50.0.0.0/8** para obtener el direccionamiento IP usando VLSM para todas las conexiones entre Routers y además teniendo los siguientes requisitos:

LAN R1: 2001:8::0/64
LAN R4: 2001:8::0/64
TUNNEL0: 2000:D::0/64

DIAGRAMA DE TOPOLOGIA

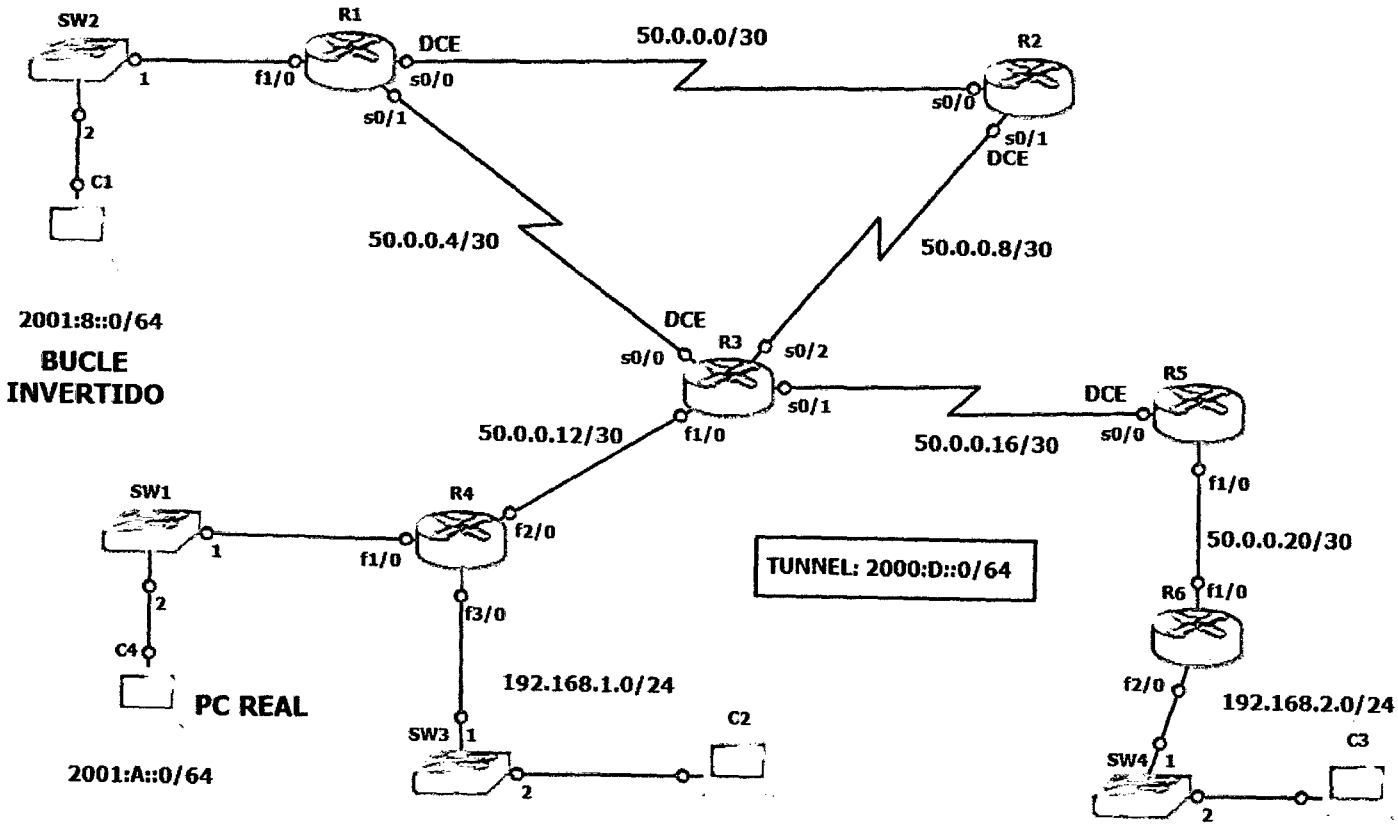


Fig. 4.17.1 Red Virtual en GNS3

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s0/0	50.0.0.5	255.255.255.252	No aplicable
	s0/1	50.0.0.1	255.255.255.252	No aplicable
	f1/0	2001:8::1	/64	No aplicable
R2	s0/0	50.0.0.2	255.255.255.252	No aplicable
	s0/1	50.0.0.9	255.255.255.252	No aplicable
R3	s0/0	50.0.0.6	255.255.255.252	No aplicable
	s0/1	50.0.0.17	255.255.255.252	No aplicable
	s0/2	50.0.0.10	255.255.255.252	No aplicable
	f1/0	50.0.0.13	255.255.255.252	No aplicable
R4	f1/0	50.0.0.14	255.255.255.252	No aplicable
	f2/0	2001:A::1	/64	No aplicable
	f3/0	192.168.1.1	255.255.255.0	No aplicable
R5	s0/0	50.0.0.18	255.255.255.252	No aplicable
	f2/0	50.0.0.21	255.255.255.252	No aplicable
R6	f1/0	50.0.0.22	255.255.255.252	No aplicable
	f2/0	192.168.2.1	255.255.255.0	No aplicable
C1	BUCLE INVERTIDO	2001:8::2	/64	2001:8::1
C2	VPCS	192.168.1.2	255.255.255.0	192.168.1.1
C3	VPCS	192.168.2.2	255.255.255.0	192.168.2.1
C4	NIC	2001:A::2	/64	2001:A::1

Tabla 4.17.1 Direccionamiento IP para las Redes

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

Montar y conectar la red igual a la del Diagrama de topología.

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

Ingrese al modo privilegiado

Router>enable

Aparece el siguiente prompt

Router#

En el modo exec privilegiado, ingrese al modo de configuración global:

Router# **configure terminal**

PASO 1: Establezca la configuración global del nombre de host.

Ingrese el siguiente comando para configurar el nombre del router:

Router(config)#**hostname XXXXXX** (Escribir nombre deseado)

PASO 2: Desactive la búsqueda DNS.

Router(config)# **no ip-domain lookup**

Si escribes algo que no sea un comando de Cisco IOS o cometes un error, el router asume que ha escrito un nombre de dominio y trata de resolver lo que usted escribe, realizando una búsqueda de DNS.

PASO 3: Configure un mensaje para que se muestre al ingresar al router.

Router(config)#**banner motd %** Solo acceso a personal autorizado **%** (Puede escribir cualquier mensaje)

El símbolo % indica el inicio y final del mensaje.

PASO 4: Configure las contraseñas de consola, enable secret y VTY.

Seguir los siguientes pasos:

Router(config)# **line console 0**

Router(config-line)# **password XXXXX** (Escribir contraseña deseada)

Router(config-line)# **login**

Router(config-line)# **exit**

Router(config)# **enable secret XXXXX** (Escribir contraseña deseada)

Router(config)# **line vty 0 4**

Router(config-line)# **password XXXXX** (Escribir contraseña deseada)

Router(config-line)# **login**

Router(config-line)# **exit**

PASO 5: Sincronice los mensajes no solicitados y el resultado de la depuración con el resultado solicitado y los indicadores para las líneas de consola y de terminal virtual.

Router(config)# **line console 0**

Router(config)# **logging synchronous**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **logging synchronous**

Router(config)# **exit**

PASO 6: Configure un tiempo de espera EXEC de 10 minutos.

Router(config)# **line console 0**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

Router(config)# **line console vty 0 4**

Router(config)# **exec-timeout 10**

Router(config)# **exit**

PASO 7: Guardar la configuración.

Router(config)# **copy running-config startup-config**

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET CON IPV4.

TAREA 4: CONFIGURAR IPV6.

Se deben configurar los Routers R1 y R4 ya que ellos recibirán los paquetes IPV6.

R1:

R1(config)# **ipv6 unicast-routing**

R1(config)# **int f2/0**

R1(config-if)# **ipv6 address 2001:8::1/64**

R1(config-if)# **ipv6 enable**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R4:

R4(config)# **ipv6 unicast-routing**

R4(config)# **int f2/0**

R4(config-if)# **ipv6 address 2001:A::1/64**

R4(config-if)# **ipv6 enable**

R4(config-if)# **no shutdown**

R4(config-if)# **exit**

PASO 2: Configurar Tunnel.

R1:

R1# **configure termimal**

R1(config)# **interface tunnel 0**

R1(config-if)# **ipv6 address 2000:D::1/64**

R1(config-if)# **tunnel source 50.0.0.5**

R1(config-if)# **tunnel destination 50.0.0.14**

R1(config-if)# **tunnel mode ipv6ip**

R1(config-if)# **exit**

R4:

R4# **configure termimal**

R4(config)# **interface tunnel 0**

R4(config-if)# **ipv6 address 2000:D::2/64**

R4(config-if)# **tunnel source 50.0.0.14**

R4(config-if)# **tunnel destination 50.0.0.5**

R4(config-if)# **tunnel mode ipv6ip**

R4(config-if)# **exit**

TAREA 5: CONFIGURAR PROTOCOLO EIGRP.

R1:

R1(config)# **router eigrp 10**

R1(config-router)# **network 50.0.0.0 0.0.0.3**

R1(config-router)# **network 50.0.0.4 0.0.0.3**

R1(config-router)# **no auto-summary**

R1(config-router)# **exit**

R3:

R3(config)# **router eigrp 10**

R3(config-router)# **network 50.0.0.4 0.0.0.3**

R3(config-router)# **network 50.0.0.8 0.0.0.3**

R3(config-router)# **network 50.0.0.12 0.0.0.3**

R3(config-router)# **network 50.0.0.16 0.0.0.3**

R3(config-router)# **no auto-summary**

R3(config-router)# **exit**

NOTA: Seguir los mismos pasos para los demás Routers con sus respectivas redes.

TAREA 6: CONFIGURAR PROTOCOLO RIPNG.

R1:

R1# **configure terminal**

R1(config)# **ipv6 router rip UNPRG**

R1(config-rtr)# **exit**

R4:

R4# **configure terminal**

R4(config)# **ipv6 router rip UNPRG**

R4(config-rtr)# **exit**

NOTA: También deberá configurarse en la interface tunnel 0, en R1 y R4.

R1# **configure termimal**

R1(config)# **interface tunnel 0**

R1(config)# **ipv6 router rip UNPRG**

Habilitar la interface del Router que aceptará los paquetes IPV6.

R1:

R1# **configure terminal**

R1(config)# **int f1/0**

R1(config-if)# **ipv6 rip UNPRG enable**

R1(config-if)# **exit**

R4:

R4# **configure terminal**

R4(config)# **int f2/0**

R4(config-if)# **ipv6 rip UNPRG enable**

R(config-if)# **exit**

TAREA 7: CONFIGURAR LOS EQUIPOS DE HOST.

BUCLE INVERTIDO

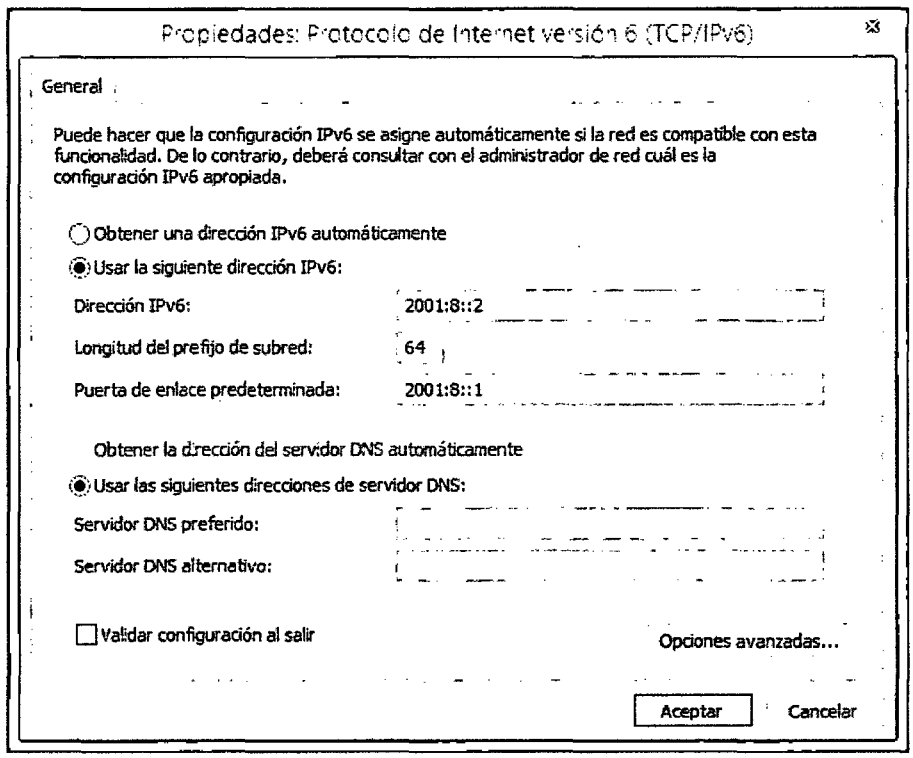


Fig. 4.17.2 Configuración de IP para BUCLE INVERTIDO.

VPCS

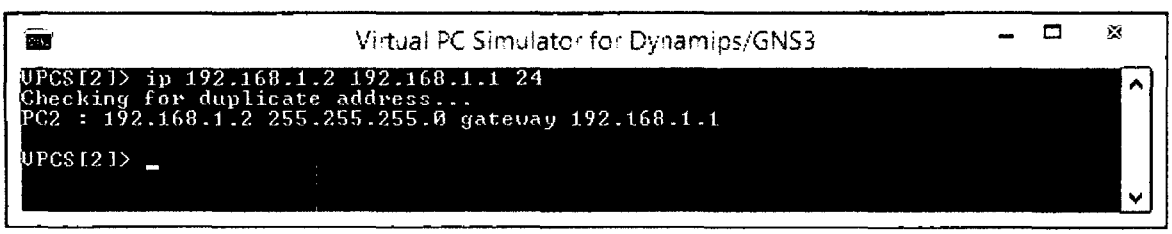


Fig. 4.17.3 Configuración de IP para VPCS.

NOTA: Configurar los demás host.

TAREA 8: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

PASO 1: Verificar configuraciones.

R1#show ipv6 route

Muestra el contenido de la tabla de enrutamiento IPV6.

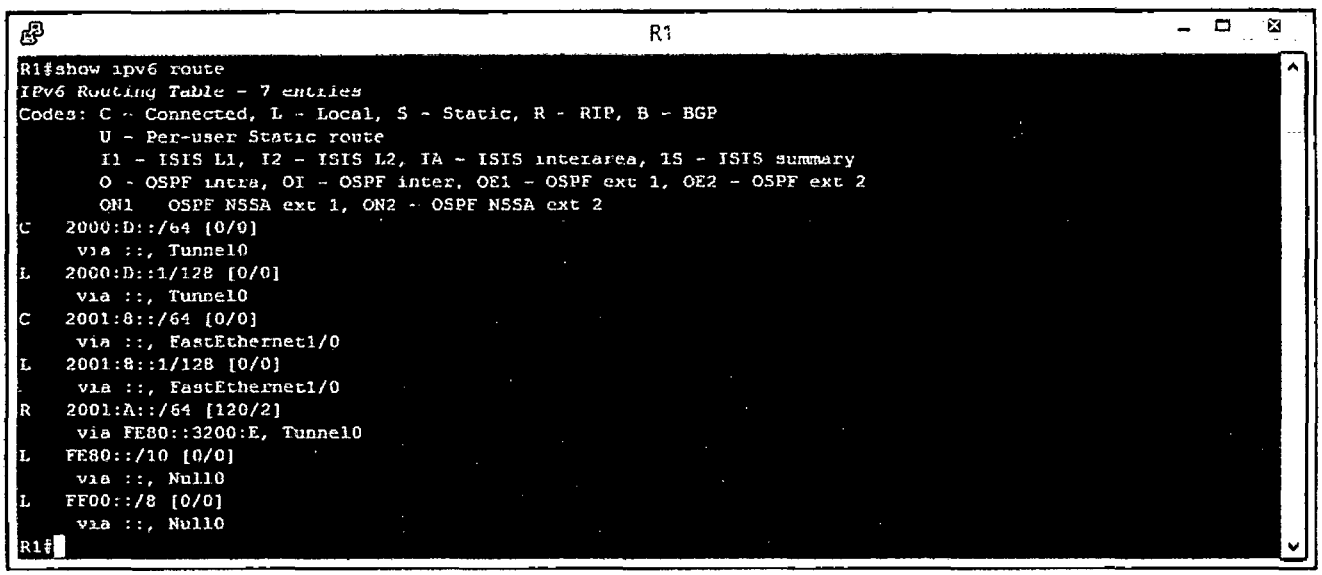


Fig. 4.17.4 Tabla de enrutamiento IPV6 de R1.

R1#show ipv6 protocols

Permite visualizar los parámetros y el estado actual de los procesos de protocolo de enrutamiento IPv6 activas

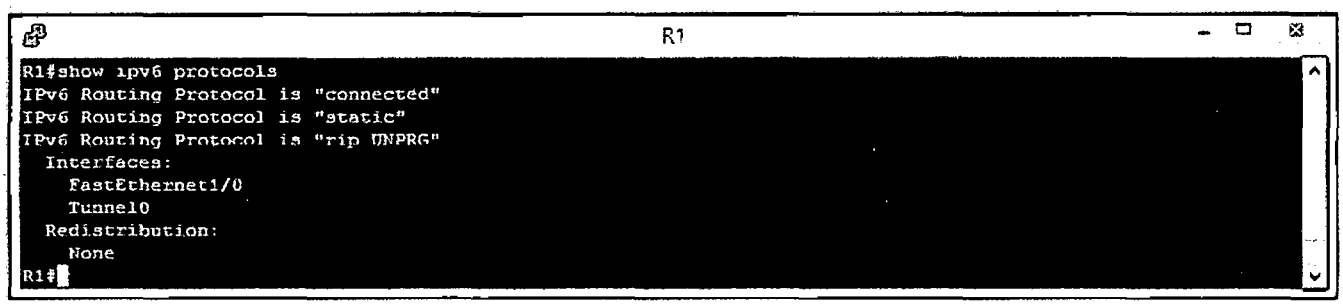


Fig. 4.17.5 Tabla de ipv6 protocols de R1.

R1#show ipv6 tunnel

Muestra información del tunnel IPV6.

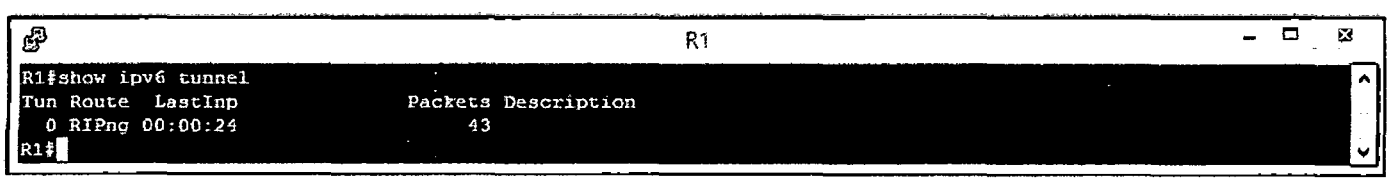


Fig. 4.17.6 Tabla ipv6 tunnel de R1.

R1#show ip protocols

```
R1#show ip protocols
Routing Protocol is "eigrp 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 10
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    50.0.0.0/30
    50.0.0.4/30
  Routing Information Sources:
    Gateway         Distance      Last Update
    50.0.0.2              90      00:08:55
    50.0.0.6              90      00:08:55
  Distance: internal 90 external 170

R1#
```

Fig. 4.17.7 Tabla de ipv6 protocols de R1.

R1#show ipv6 interface

Muestra el estado de las interfaces configurado con IPV6.

```
R1#show ipv6 interface
FastEthernet1/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::CE02:EFF:FE7C:10
  Global unicast address(es):
    2001:8::1, subnet is 2001:8::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::9
    FF02::1:FF00:1
    FF02::1:FF7C:10
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
Tunnel0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::3200:5
  Global unicast address(es):
    2000:D::1, subnet is 2000:D::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::9
    FF02::1:FF00:1
    FF02::1:FF00:5
  MTU is 1480 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  Hosts use stateless autoconfig for addresses.
R1#
```

Fig. 4.17.8 Tabla de ipv6 interface de R1.

PASO 2: Utilice el comando ping para probar la conectividad entre los routers que *no están directamente conectados y también la conectividad entre host.*

PING ENTRE ROUTERS

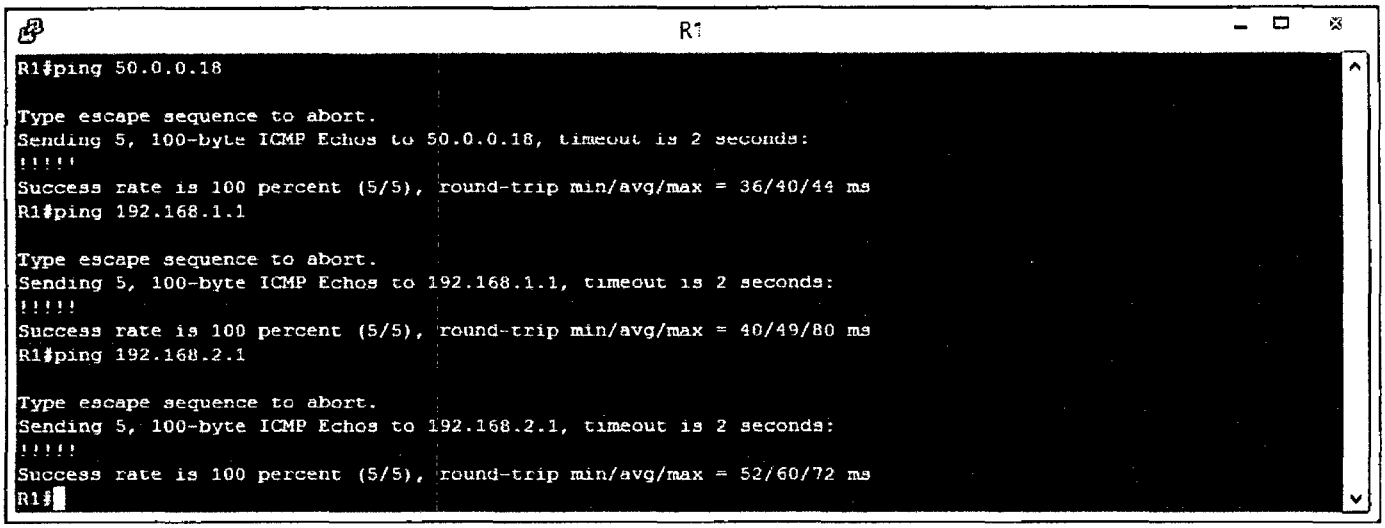


Fig. 4.17.9 Prueba de conectividad entre routers.

BUCLE INVERTIDO

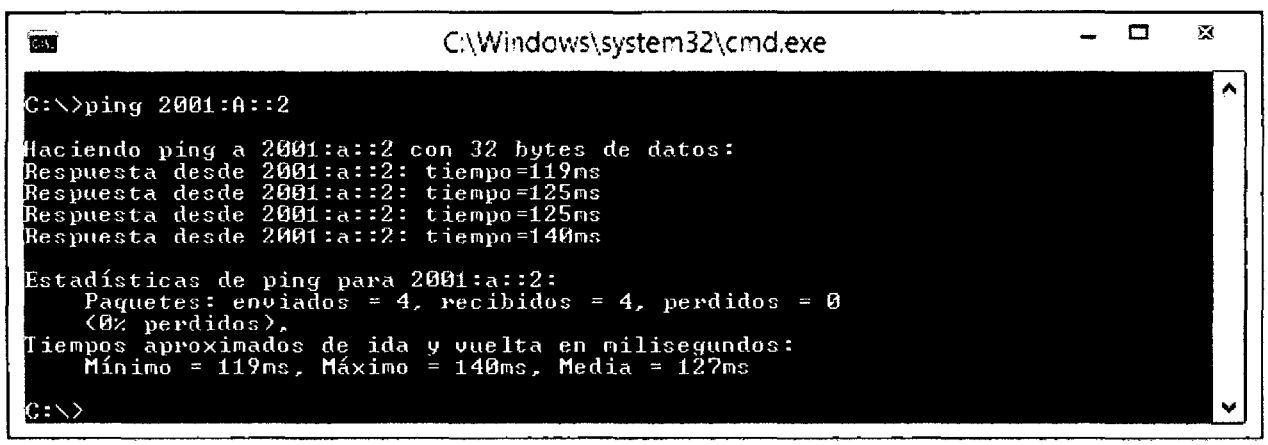


Fig. 4.17.10 Prueba de conectividad entre routers.

NOTA: Configurar los demás host.

TAREA 9: ANALIS DEL TRAFICO DE PAQUETES.

PASO 1: Medición de la Latencia

Para la medición de la latencia se realizó 10 muestras sucesivas de 100 ping desde el C1 (Bucle invertido) hacia la PC REAL considerando un tamaño de trama de 64, 512 y 1518 bytes como se especifica en el RFC 2544.

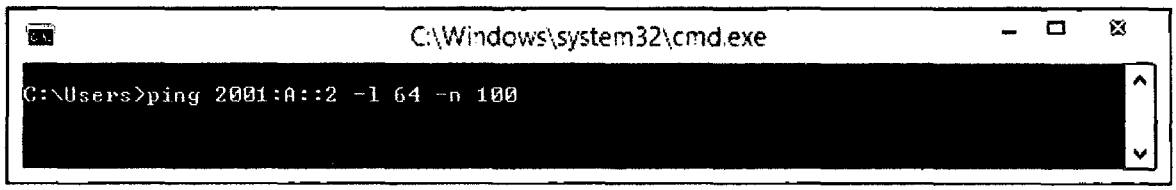


Fig. 4.17.11 Prueba de conectividad entre routers.

En la Figura 4.17.11 se puede observar el envío de 100 ping con una trama de 1518 hacia la dirección 2001:A::2

En las Tablas posteriores se detallan los valores de la Latencia que se ha obtenido una vez realizadas todas las muestras.

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	**68**	**67**	**61**	**62**	**62**	**61**	**65**	**59**	**60**	**64**	**62.9**
Tiempo Máximo (ms)	**168**	**355**	**102**	**133**	**117**	**355**	**106**	**120**	**111**	**111**	**167.8**
Tiempo Promedio (ms)	**86**	**96**	**80**	**87**	**81**	**99**	**84**	**84**	**79**	**86**	**86.2**

Tabla 4.17.2 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	512										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	56	62	60	58	60	58	59	69	59	61	64.7
Tiempo Máximo (ms)	106	116	114	109	102	120	123	129	107	107	113.3
Tiempo Promedio (ms)	80	85	82	82	82	88	88	87	85	89	89.3

Tabla 4.17.3 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1518										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	61	64	70	62	67	75	75	70	72	77	69.3
Tiempo Máximo (ms)	393	107	122	117	117	110	101	114	108	117	140.6
Tiempo Promedio (ms)	101	88	97	86	88	93	92	95	88	93	92.1

Tabla 4.17.4 Datos obtenidos para una trama de 1518 bytes.

LATENCIA			
Tamaño de Trama (bytes)	64	512	1518
Tiempo Mínimo (ms)	62.9	64.7	69.3
Tiempo Máximo (ms)	167.8	113.3	140.6
Tiempo Promedio (ms)	86.2	89.3	92.1

Tabla 4.17.5 Comparación de datos obtenidos de las diferentes tramas.

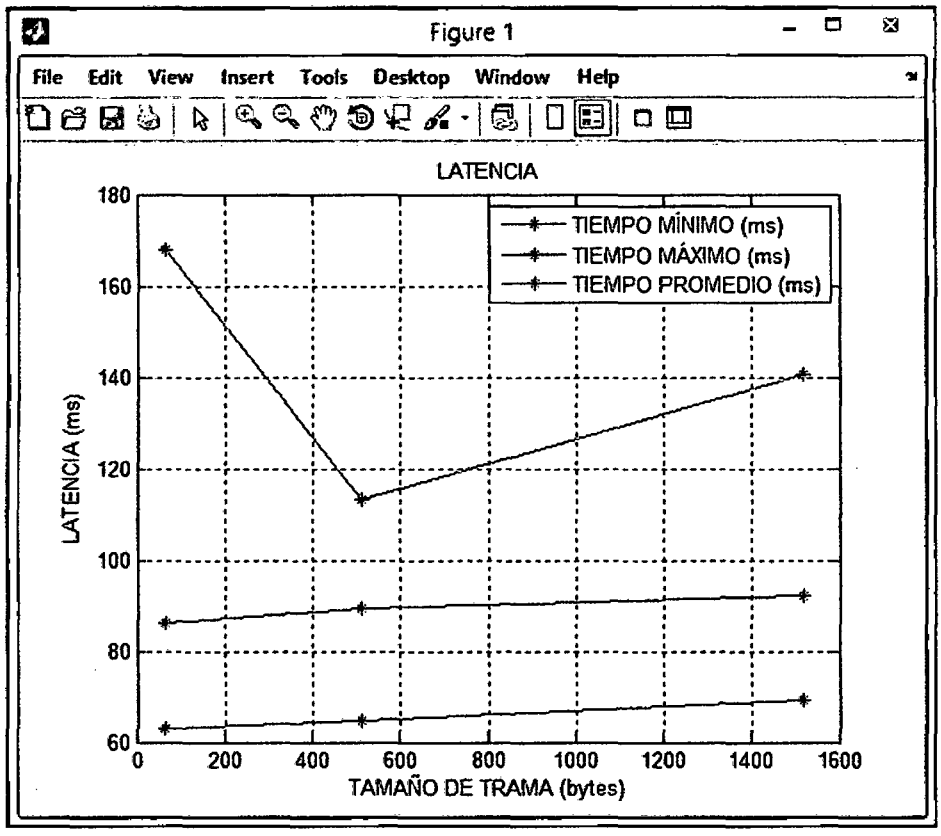


Fig. 4.17.12 Datos representados gráficamente de la variación de la latencia.

De acuerdo con los datos obtenidos, se puede observar claramente que los valores mínimo (color azul), máximo (color rojo) y promedio (color verde) de la latencia de la red se incrementan conforme se envía una trama de longitud mayor, en este caso con la trama de 1518 bytes se obtiene una latencia promedio de 92.1 ms a diferencia de una trama de 64 bytes con 86.2 ms.

PASO 2: Medición del Throughput

Para la medición del Throughput y Jitter se envió una cantidad de tramas a velocidades diferentes durante 20 segundos, hasta encontrar la máxima cantidad de tramas recibidas sin que se produzcan perdidas de las mismas en el router y PC REAL. Como se utilizó Jperf el cliente será el encargado de enviar los paquetes y el servidor los recibirá, indicando la cantidad de paquetes que llegaron correctamente considerando un tamaño del paquete UDP de 750, 1125, 1500 y 1470 (default) bytes, tal como se especifica en el RFC 768.

Configuración del Jperf como servidor con UDP Packet Size de 750 Bytes.

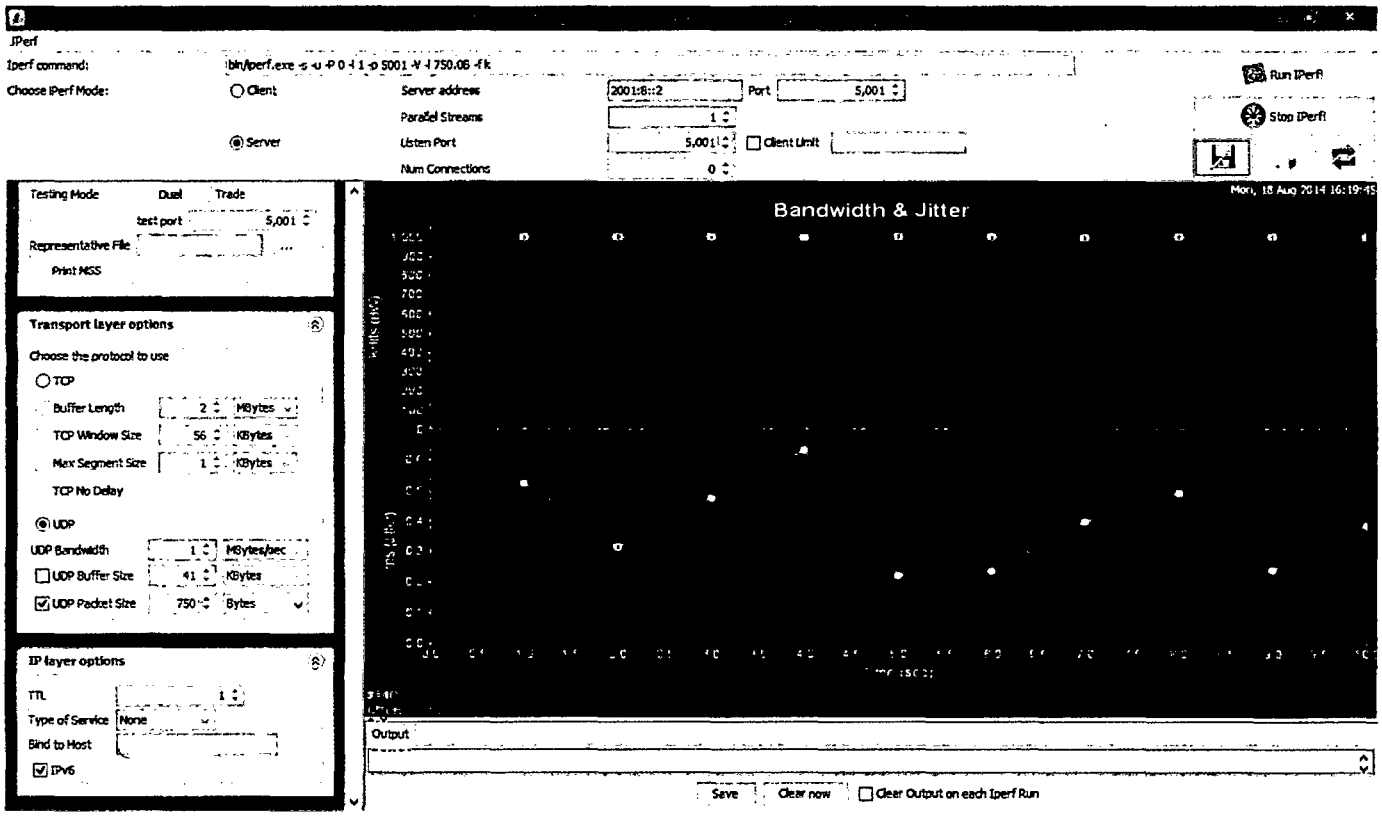
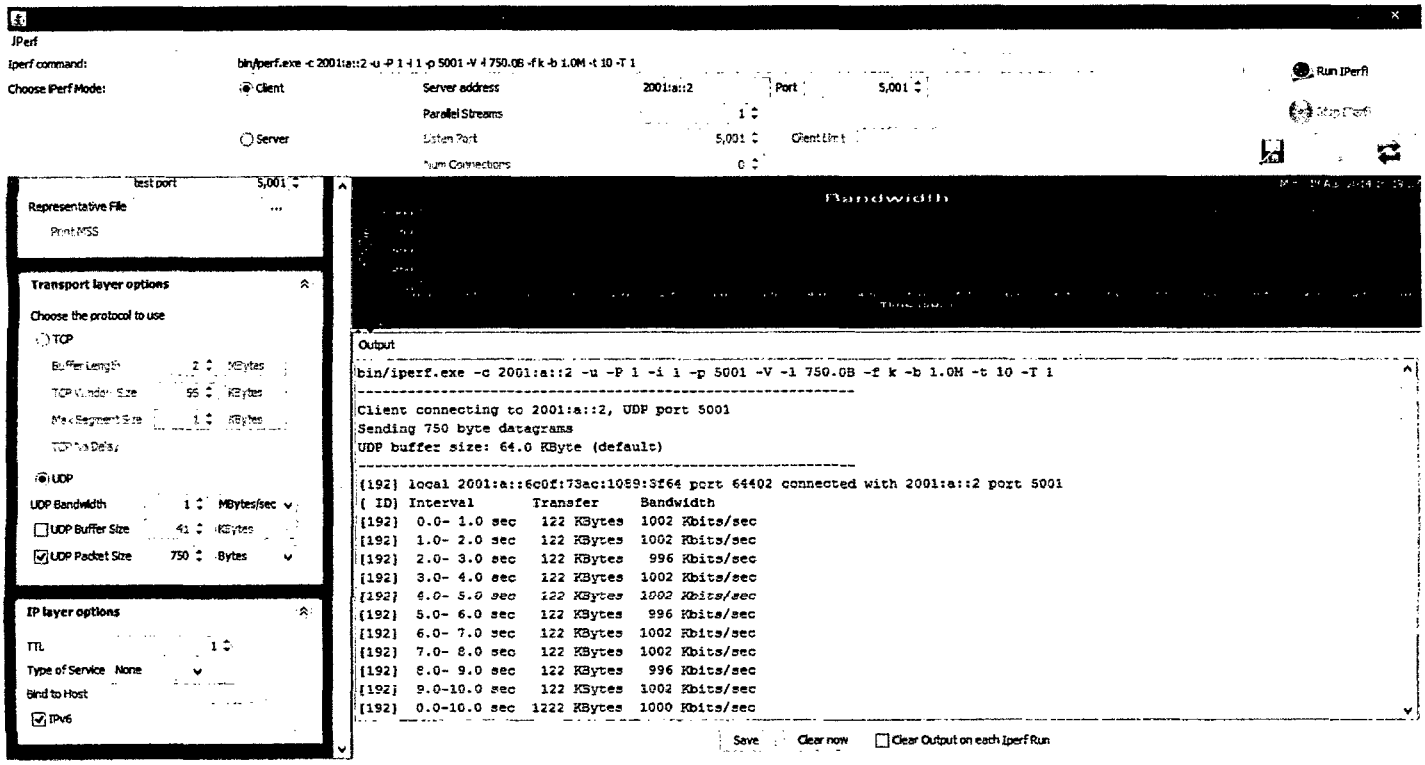


Fig. 4.17.13 Gráfica de Bandwidth y Jitter.

```
bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -V -l 750.0B -f k
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 750 byte datagrams
UDP buffer size: 64.0 KByte (default)
------------------------------------------------------------
OpenSCManager failed - Acceso denegado. (0x5)
[140] local 2001:a::ac40:9928:7a48:5465 port 5001 connected with 2001:a::6c0f:73ac:1089:3f64 port 64402
[ ID] Interval       Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[140]  0.0- 1.0 sec   122 KBytes  1002 Kbits/sec  0.522 ms 544039282/  167 (3.3e+008%)
[140]  1.0- 2.0 sec   122 KBytes  1002 Kbits/sec  0.313 ms    0/  167 (0%)
[140]  2.0- 3.0 sec   122 KBytes  1002 Kbits/sec  0.474 ms    0/  167 (0%)
[140]  3.0- 4.0 sec   122 KBytes   996 Kbits/sec  0.631 ms    0/  166 (0%)
[140]  4.0- 5.0 sec   122 KBytes  1002 Kbits/sec  0.220 ms    0/  167 (0%)
[140]  5.0- 6.0 sec   122 KBytes  1002 Kbits/sec  0.234 ms    0/  167 (0%)
[140]  6.0- 7.0 sec   122 KBytes   996 Kbits/sec  0.396 ms    0/  166 (0%)
[140]  7.0- 8.0 sec   122 KBytes  1002 Kbits/sec  0.491 ms    0/  167 (0%)
[140]  8.0- 9.0 sec   122 KBytes  1002 Kbits/sec  0.238 ms    0/  167 (0%)
[140]  9.0-10.0 sec   122 KBytes   996 Kbits/sec  0.383 ms    0/  166 (0%)
[140]  0.0-10.0 sec  1222 KBytes  1001 Kbits/sec  0.367 ms    0/ 1668 (0%)
```

Fig. 4.17.14 Resultados al medir como servidor.

Configuración del Jperf como cliente con UDP Bandwidth de 1 Mbps y UDP Packet Size



de 750 Bytes.

Fig. 4.17.15 Resultados del Jperf como Cliente.

En las siguientes Tablas se detalla los valores del Throughput obtenidos una vez realizada todas las muestras.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**1**	**1**	**1**
Velocidad de Rx (Mbps)	**1**	**1**	**1**
Tramas Transmitidas	**1668**	**1113**	**835**
Tramas Recibidas	**1668**	**1113**	**835**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**1668**	**111.3**	**83.5**

Tabla 4.17.6 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	**0.5**	**0.8**	**2**
Velocidad de Rx (Mbps)	**0.5**	**0.8**	**2**
Tramas Transmitidas	**427**	**682**	**1702**
Tramas Recibidas	**427**	**682**	**1702**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Tramas Recibidas (pps)	**42.7**	**68.2**	**170.2**

Tabla 4.17.7 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

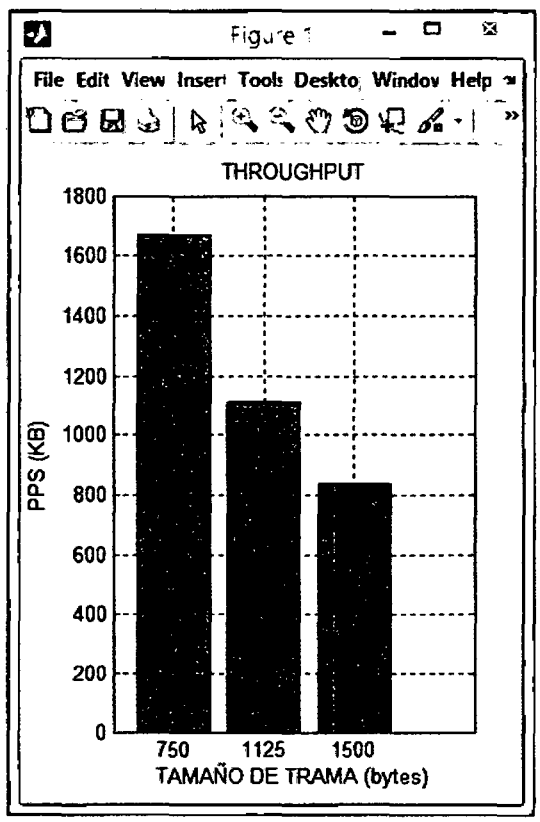


Fig. 4.17.16 PPS vs. Tamaño de Trama.

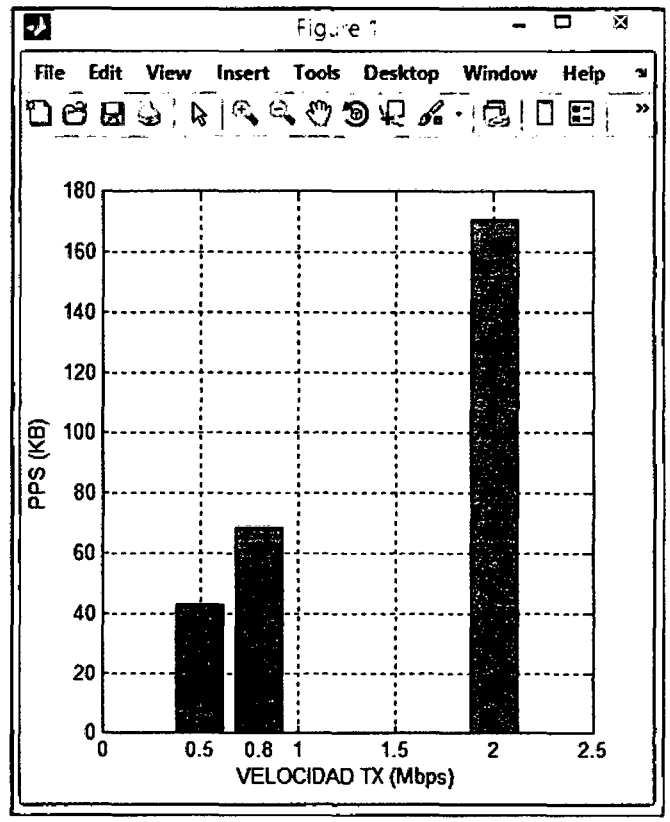


Fig. 4.17.17 PPS vs. Velocidad Tx.

En la figura 4.17.16, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 750 bytes, 1125 bytes y 1500 bytes los cuales han utilizado una velocidad de Tx constante de 1 Mbps, en la gráfica se puede observar claramente que al enviar una trama de 750 bytes se envía 1668 pps, con una trama de 1125 se envía 1113 pps y con una trama de 1500 se envía 835 pps.

Mientras en la figura 4.17.17, se representa la cantidad de paquetes enviados en un segundo al enviar tramas de 1470 bytes los cuales han utilizado una velocidad de Tx variada de: 0.5 Mbps, 0.8 Mbps y 2 Mbps, sin que se produzcan perdidas en el envío, como los datos que se muestran en la tabla 4.17.7.

PASO 3: Medición del Jitter

Para la medición se envió datos UDP de longitud variable a velocidades diferentes de Throughput obtenida anteriormente durante 20 segundos. Como se utilizó anteriormente Jperf el cliente será el encargado de enviar los datos y el servidor los recibirá, indicando los valores de Jitter obtenidos durante la transmisión de los datos.

Configuración del Jperf como servidor con UDP Packet Size por defecto.

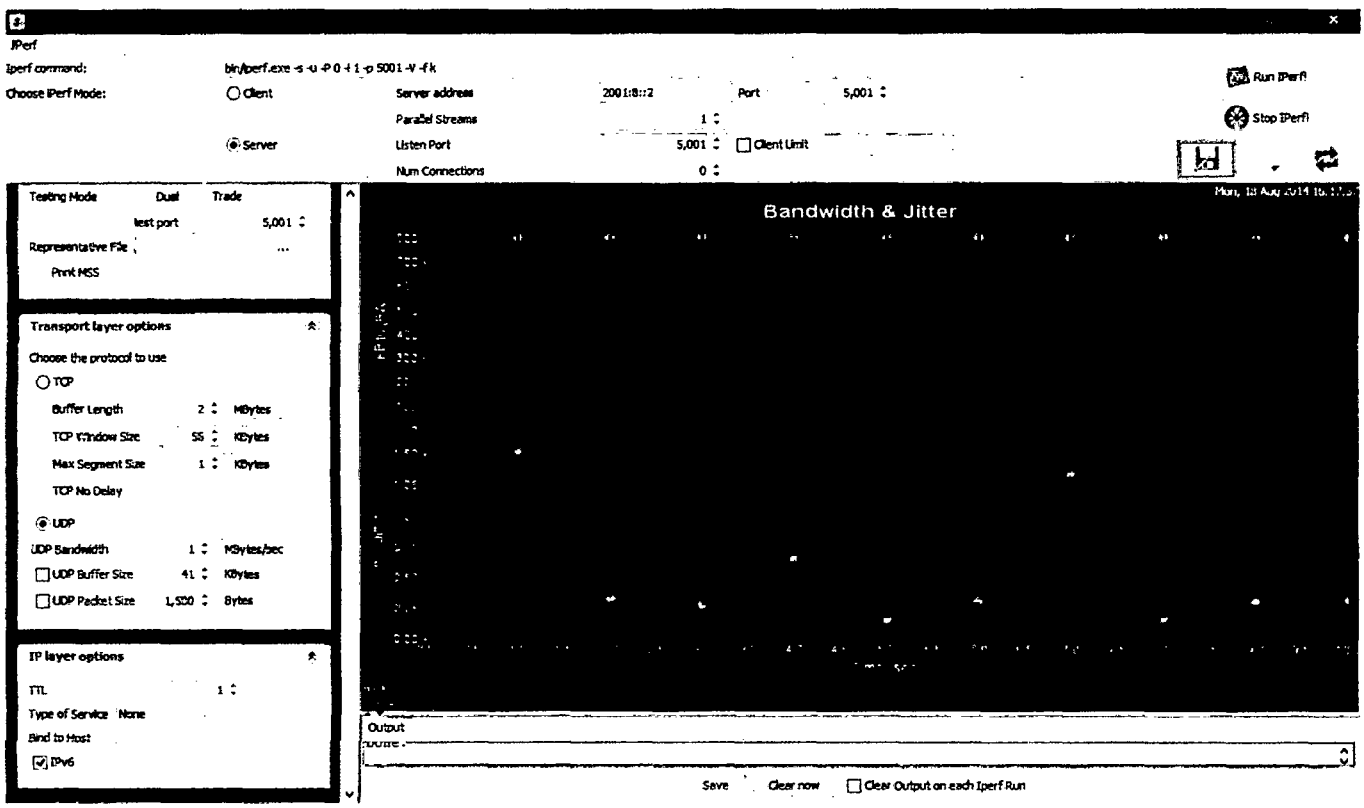


Fig. 4.17.18 Gráfica de Bandwidth y Jitter.

```
bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -V -f k
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 64.0 KByte (default)
------------------------------------------------------------
OpenSCManager failed - Acceso denegado. (0x5)
[140] local 2001:a::ac40:9928:7a48:5465 port 5001 connected with 2001:a::6c0f:73ac:1089:3f64 port 61627
[ ID] Interval       Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[140]  0.0- 1.0 sec  97.6 KBytes   800 Kbits/sec  1.526 ms    0/   68 (0%)
[140]  1.0- 2.0 sec  97.6 KBytes   800 Kbits/sec  0.335 ms    0/   68 (0%)
[140]  2.0- 3.0 sec  97.6 KBytes   800 Kbits/sec  0.287 ms    0/   68 (0%)
[140]  3.0- 4.0 sec  97.6 KBytes   800 Kbits/sec  0.651 ms    0/   68 (0%)
[140]  4.0- 5.0 sec  97.6 KBytes   800 Kbits/sec  0.155 ms    0/   68 (0%)
[140]  5.0- 6.0 sec  97.6 KBytes   800 Kbits/sec  0.317 ms    0/   68 (0%)
[140]  6.0- 7.0 sec  97.6 KBytes   800 Kbits/sec  1.342 ms    0/   68 (0%)
[140]  7.0- 8.0 sec  97.6 KBytes   800 Kbits/sec  0.164 ms    0/   68 (0%)
[140]  8.0- 9.0 sec  97.6 KBytes   800 Kbits/sec  0.312 ms    0/   68 (0%)
[140]  9.0-10.0 sec  97.6 KBytes   800 Kbits/sec  0.315 ms    0/   68 (0%)
[140]  0.0-10.0 sec   979 KBytes   800 Kbits/sec  0.335 ms    0/  682 (0%)
```

Fig. 4.17.19 Resultados al medir como servidor.

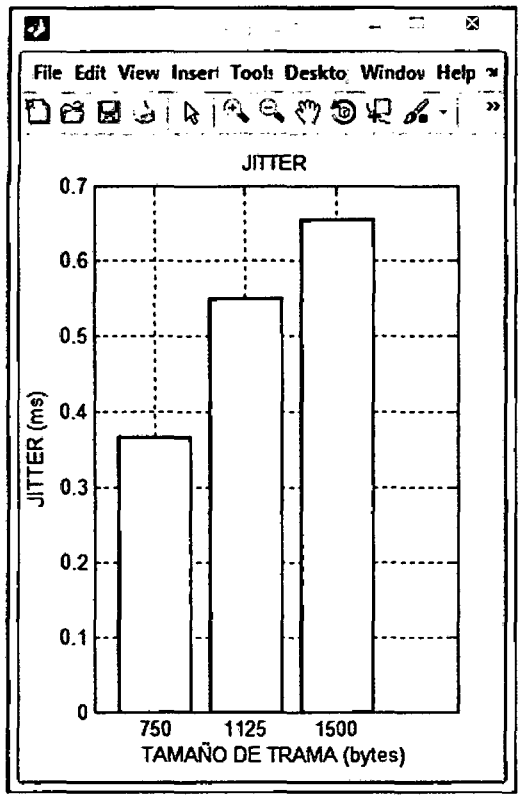
En las siguientes Tablas se detalla los valores del Jitter obtenidos una vez realizada todas las muestras.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	**1**	**1**	**1**
Velocidad de Rx (Mbps)	**1**	**1**	**1**
Tramas Transmitidas	**1668**	**1113**	**835**
Tramas Recibidas	**1668**	**1113**	**835**
Tramas Perdidas	**0 (0%)**	**0 (0%)**	**0 (0%)**
Jitter (ms)	**0.367**	**0.552**	**0.657**

Tabla 4.17.8 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	1470	1470	1470
Velocidad de Tx (Mbps)	0.5	0.8	2
Velocidad de Rx (Mbps)	0.5	0.8	2
Tramas Transmitidas	427	682	1702
Tramas Recibidas	427	682	1702
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	0.058	0.335	1.810

Tabla 4.17.9 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.



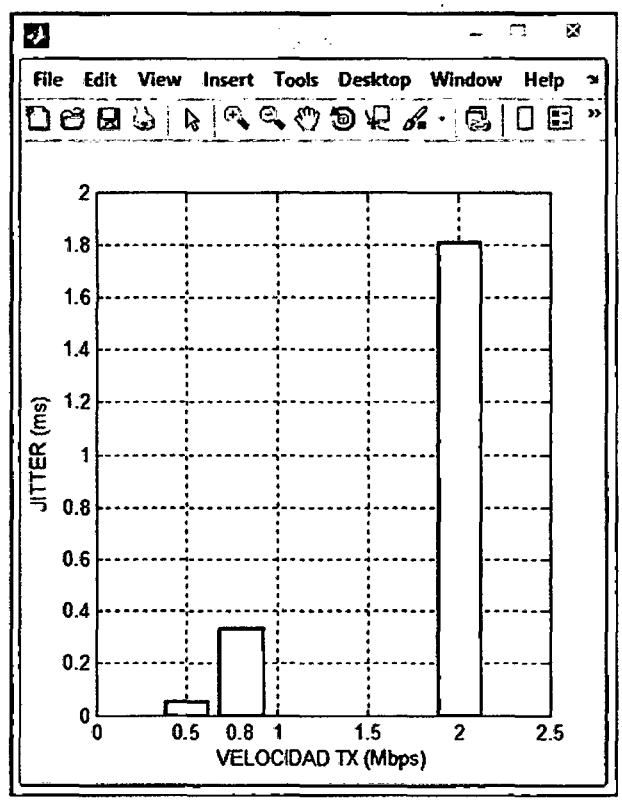


Fig. 4.17.20 Jitter vs. Tamaño de Trama Tx

Fig. 4.17.21 Jitter vs. Velocidad

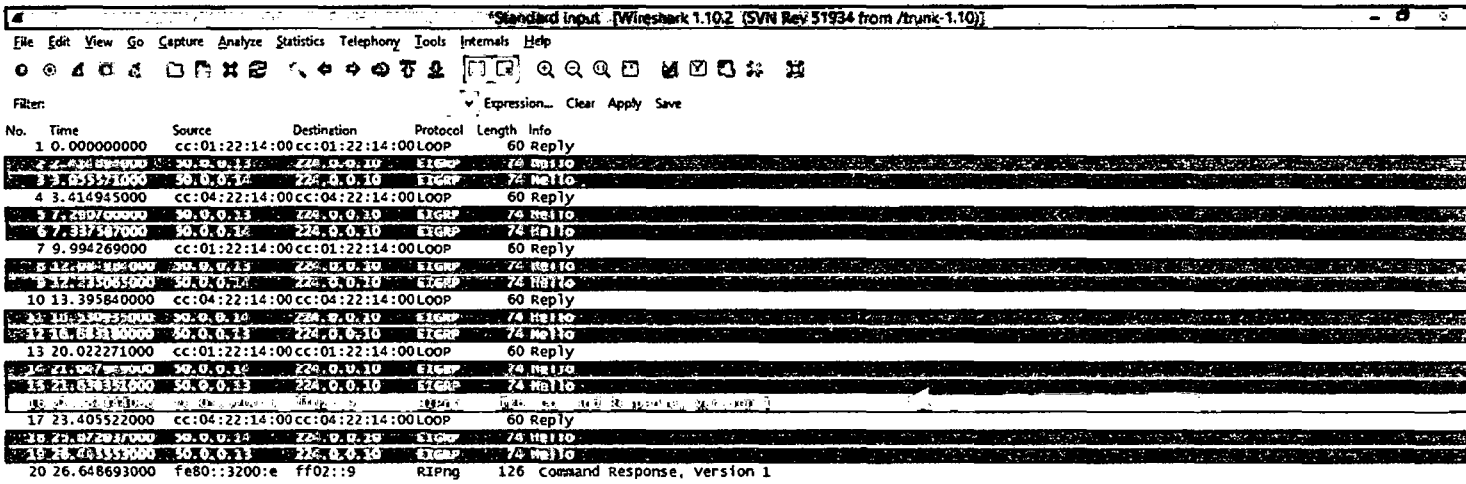
En la figura 4.17.20 se observa los valores del Jitter obtenidos al enviar diferentes tamaños de paquete UDP como 750, 1125 y 1500 bytes utilizando una velocidad de Tx constante de 1 Mbps, se puede observar claramente que con una trama de 750 bytes se tiene un Jitter de 0.367 ms a diferencia de la trama de 1500 bytes en la cual se tiene un Jitter de 0.657 ms.

En la figura 4.17.21, se observa los valores del Jitter obtenidos al enviar paquetes UDP de 1470 bytes utilizando una velocidad de Tx que varía de: 0.5 Mbps, 0.8 Mbps y 2 Mbps, sin que se pierdan paquetes en la red.

PASO 4: Captura de tráfico con Wireshark.

Capturar tráfico de paquetes en la interfaz f2/0 de R4.

- Captura de paquetes RIPng, enrutamiento RIP para IPV6 se rige de la RFC



2080.

Fig. 4.17.22 Captura de paquete RIPng con Wireshark.

En esta imagen se puede observar más detalladamente, como ver el campo del tunnel

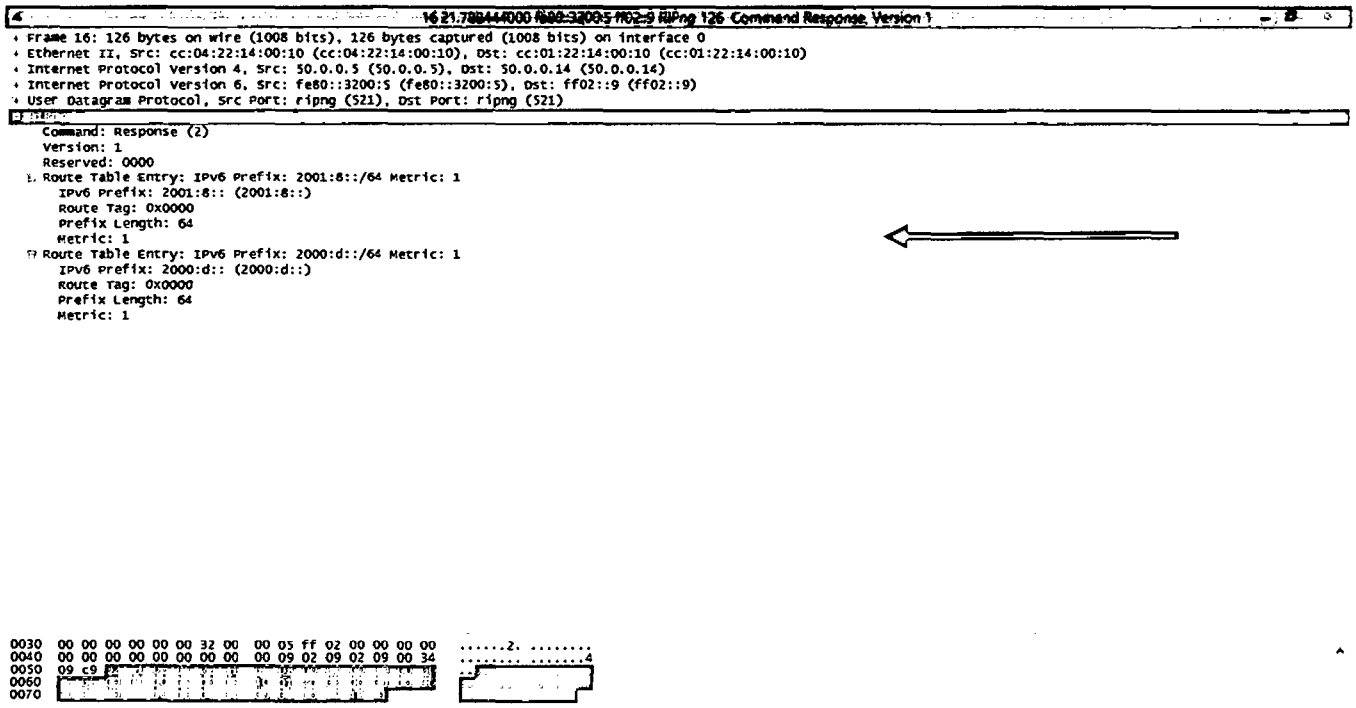


Fig. 4.17.23 Información detallada del paquete RIPng.

Información más detallada sobre Internet Protocol Version 6.

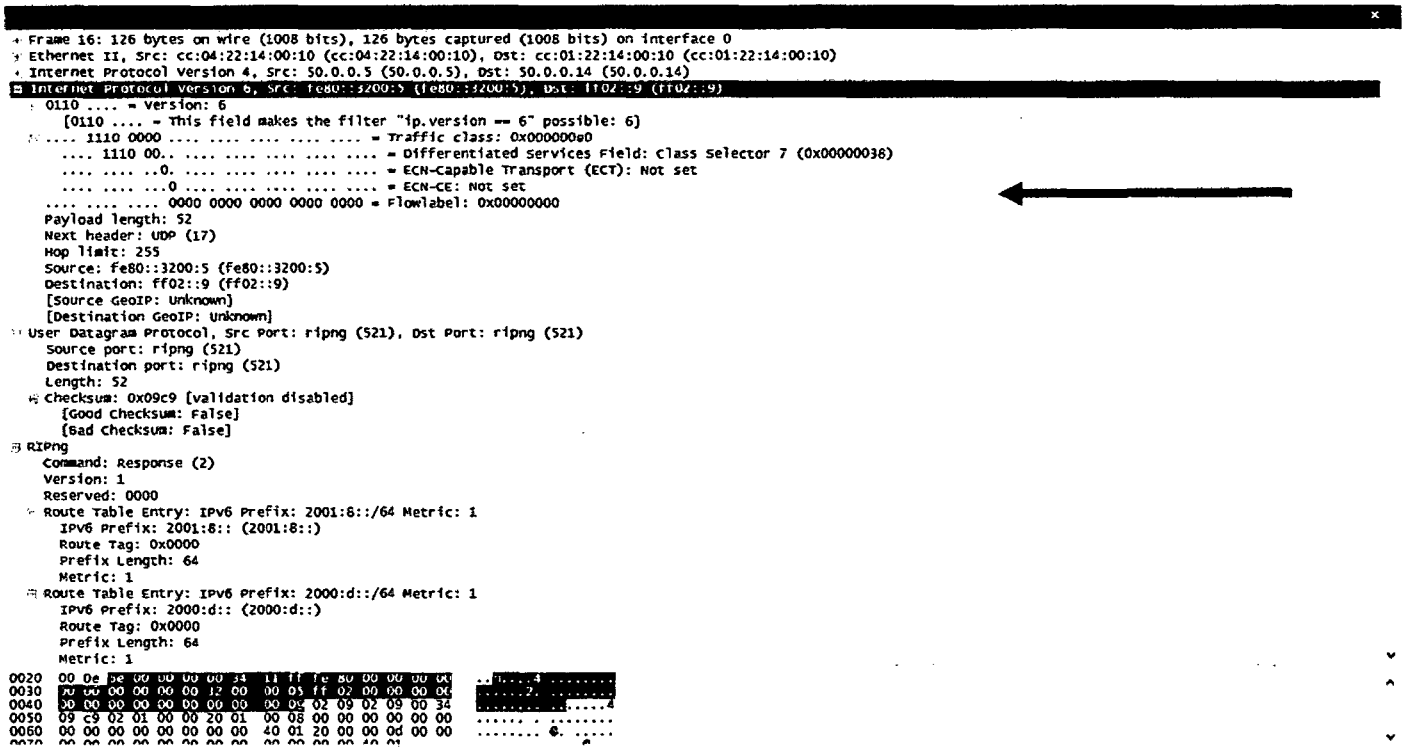


Fig. 4.17.24 Información detallada sobre Internet Protocol Version 6.

Información más detallada sobre Internet Protocol Version 4.

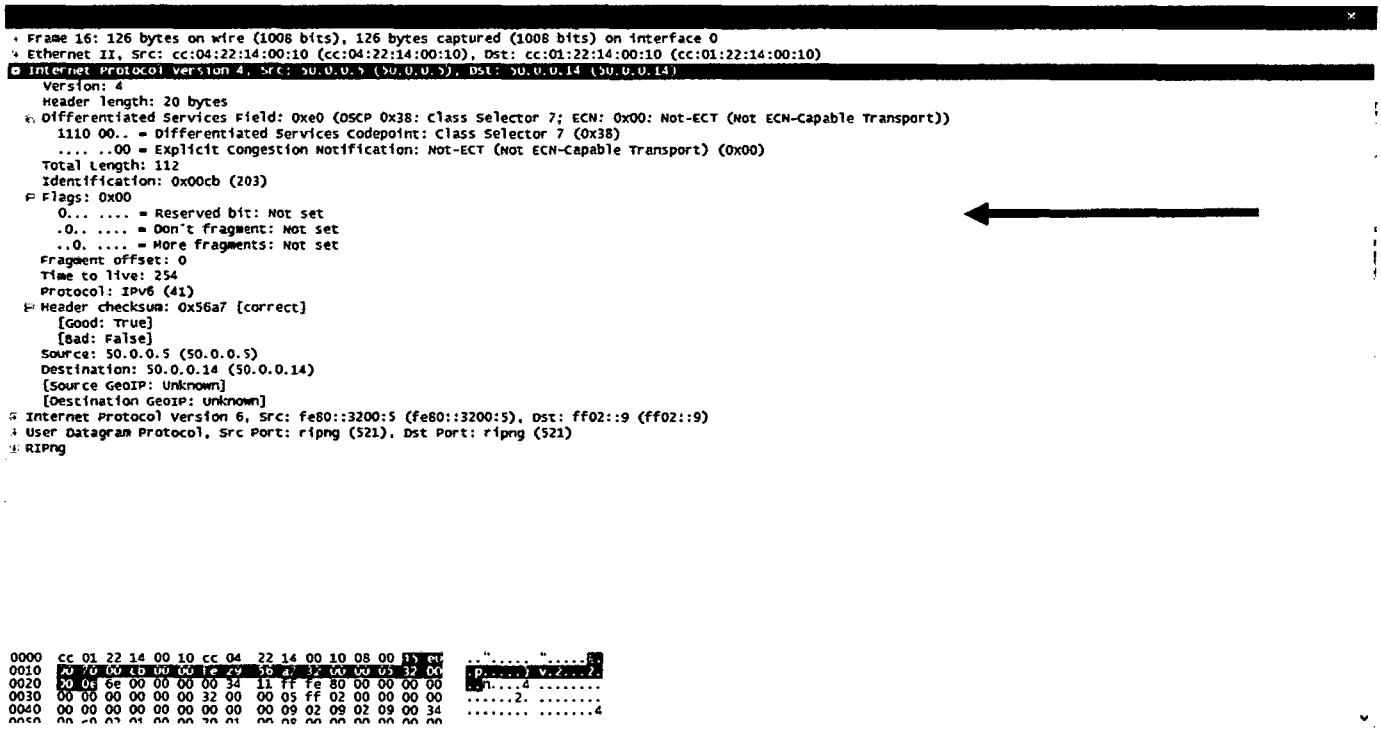


Fig. 4.17.25 Información detallada sobre Internet Protocol Version 4.

- Captura de paquetes ICMPV6, ping realizado por maquinas IPV6.

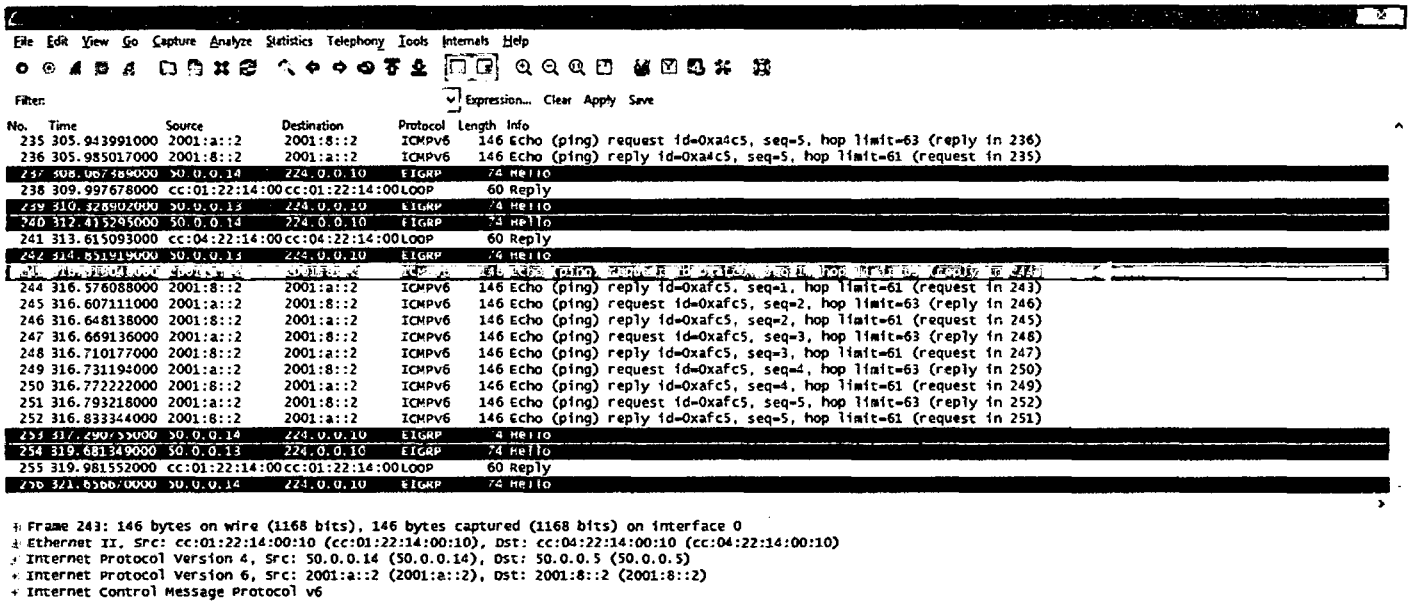


Fig. 4.17.26 Captura de paquete ICMPV6 con Wireshark.

Información más detallada sobre paquete ICMPv6:

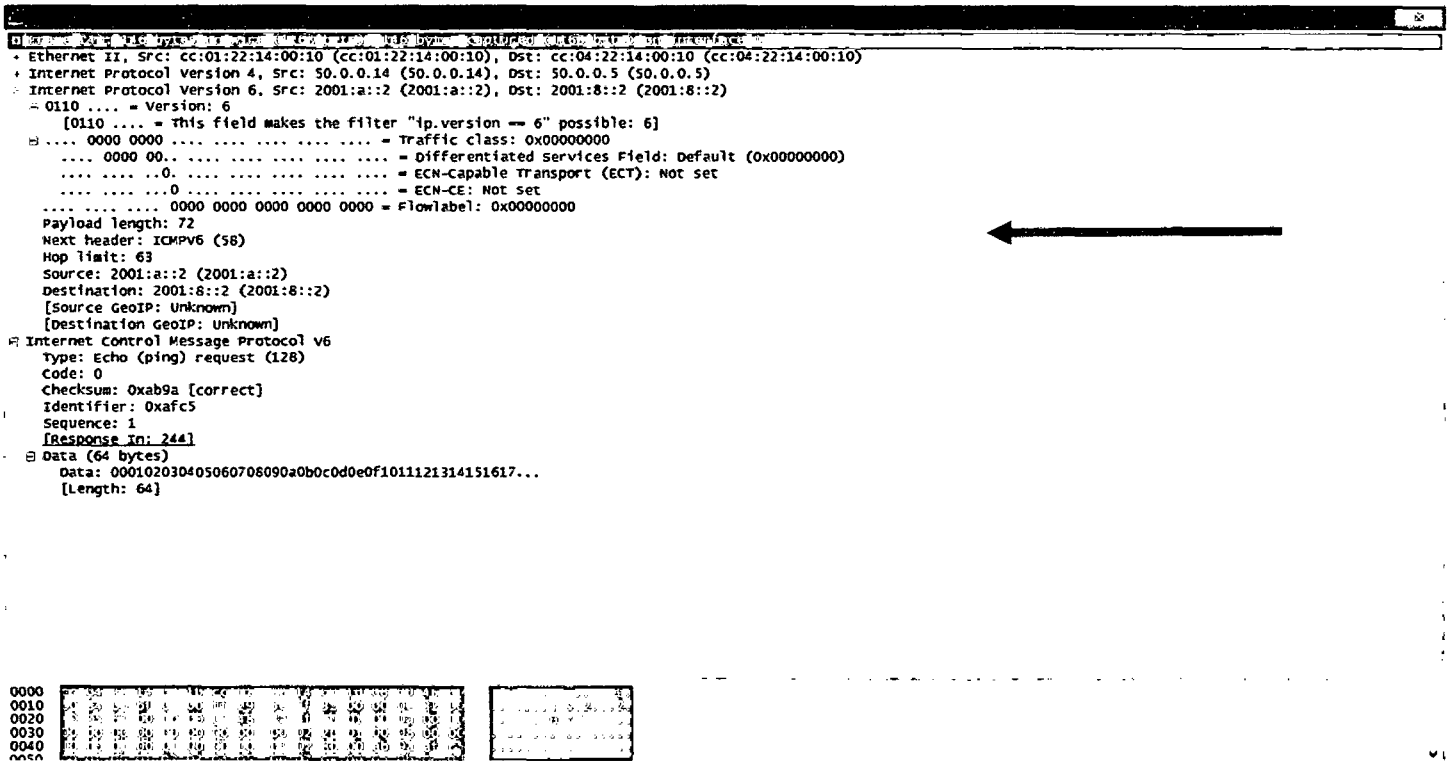


Fig. 4.17.27 Información detallada del paquete ICMPV6.

- Captura de paquetes Telnet

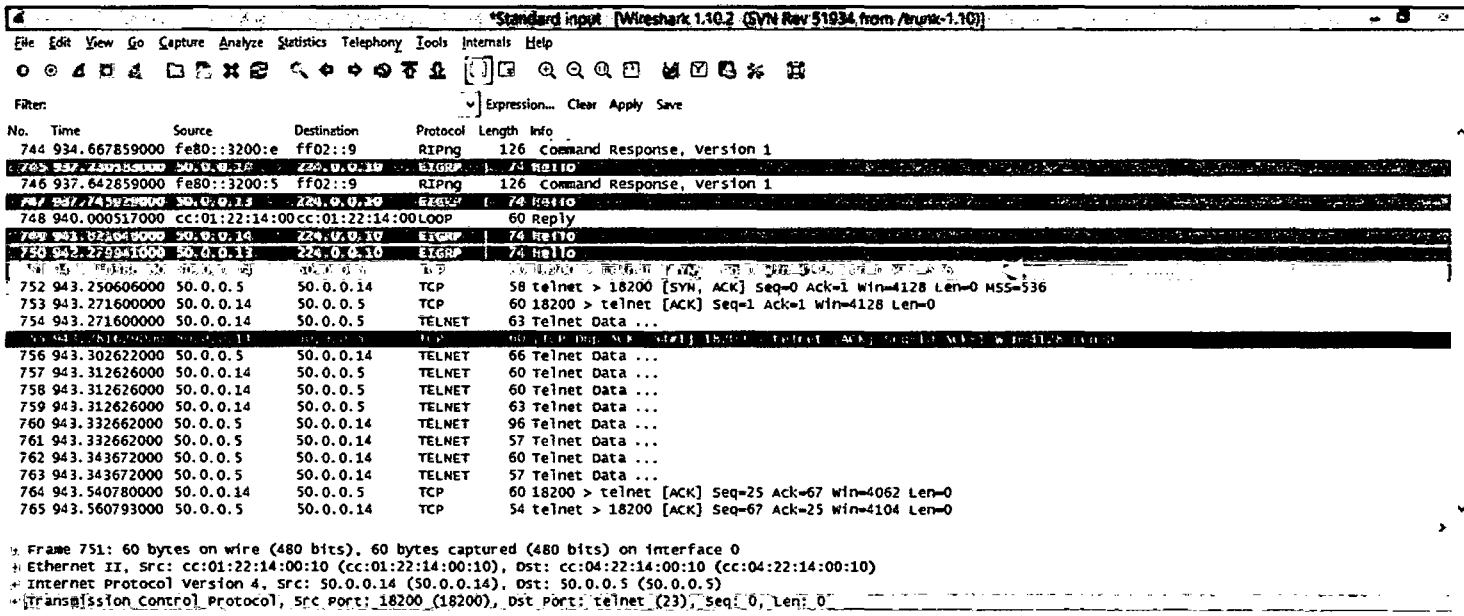


Fig. 4.17.28 Información detallada del paquete telnet con Wireshark.

CAPITULO V

DISEÑO DE DESAFÍOS DE LABORATORIO CON SIMULADOR GNS3 Y EQUIPOS FÍSICOS

DESAFIO 5.1: CONFIGURACION BASICA DE RUTAS ESTATICAS

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet y GigabitEhernet.
- Configurar una ruta estática por medio de una interfaz de salida.
- Configurar una ruta estática mediante una dirección de siguiente salto.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

DIAGRAMA DE TOPOLOGIA

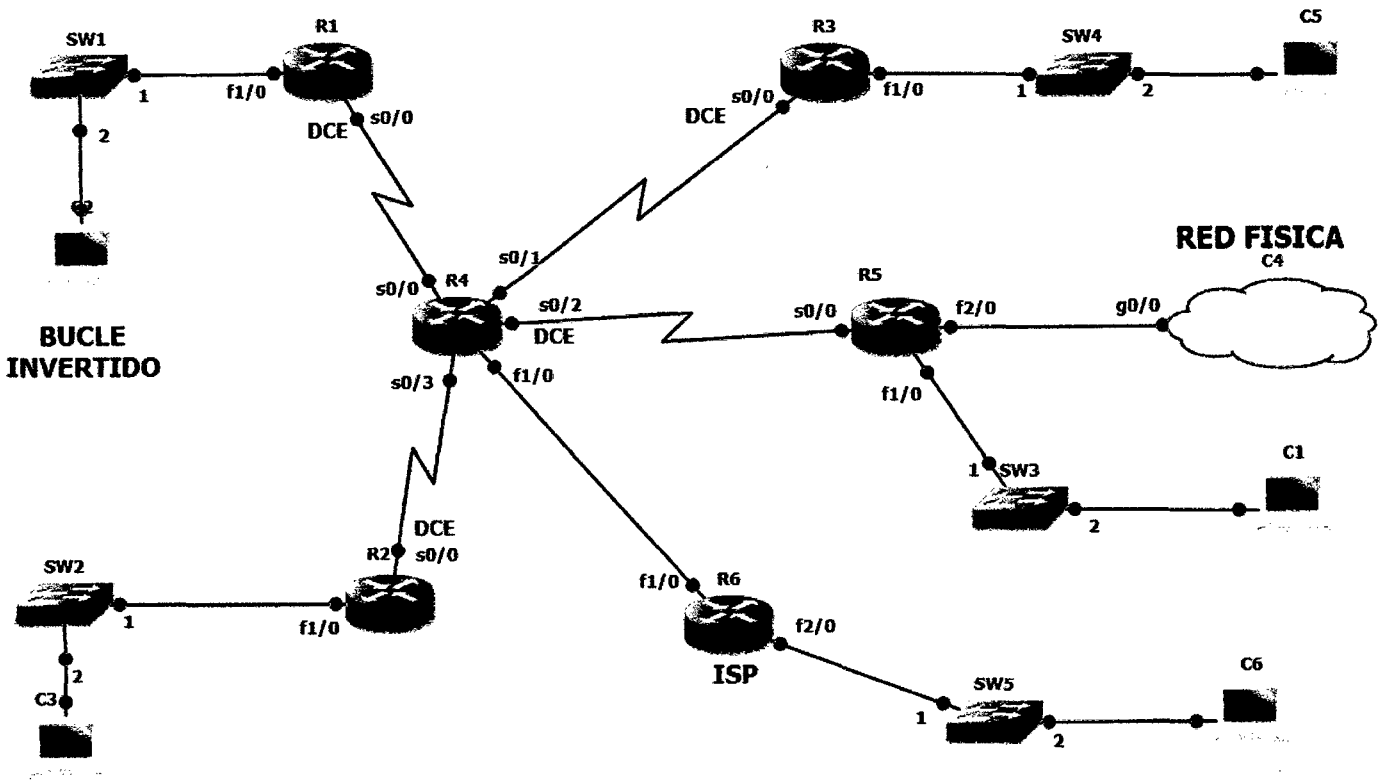


Fig. 5.1.1 Red Virtual en GNS3

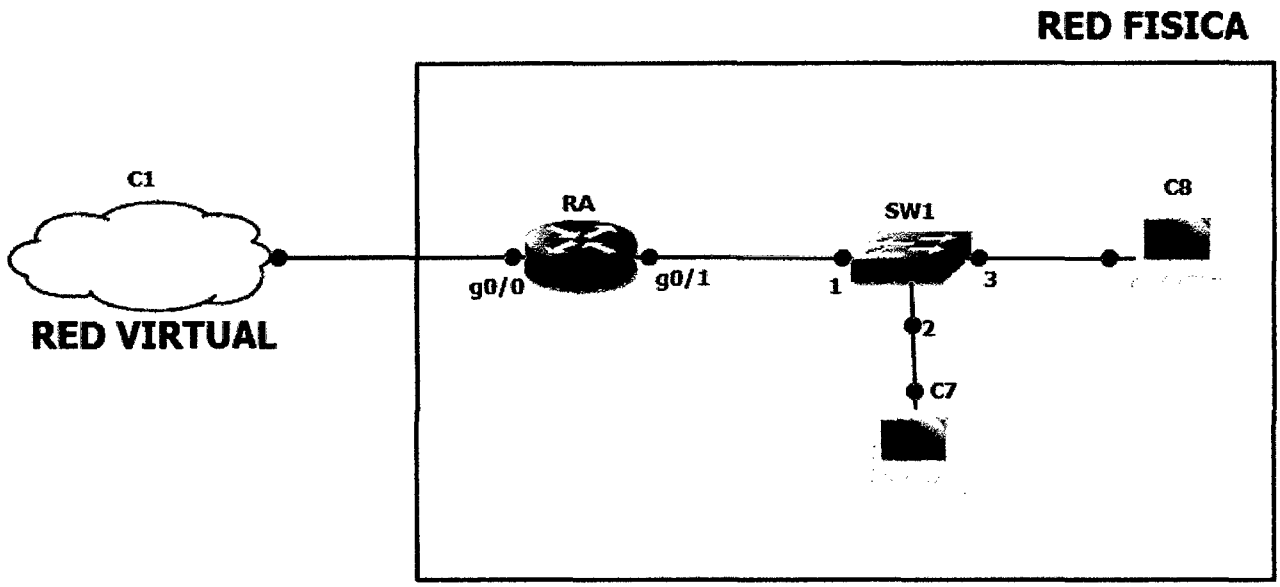


Fig. 5.1.2 Red Física.

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s0/0			
	f1/0			
R2	s0/0			
	f1/0			
R3	s0/0			
	f1/0			
R4	s0/0			
	s0/1			
	s0/2			
	s0/3			
	f1/0			
R5	s0/0			
	f1/0			
	f2/0			
R6	f1/0			
	f2/0			
RA	g0/0			
	g0/1			
C1	VPCS			
C2	BUCLE INVERTIDO			
C3	VPCS			
C5	VPCS			
C6	VPCS			
C7	NIC			
C8	NIC			

Tabla 5.1.1 Direccionamiento IP para las Redes

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **100.10.0.0/8** para obtener el direccionamiento IP usando VLSM para las conexiones entre routers, además dividir la red **192.168.1.0/24** para proporcionar direcciones para las 4 LAN:

- LAN R1: 20 host.
- LAN R2: 38 host.
- LAN R4: 40 host.
- LAN Router físico: 22 host.

PASO 1: Asignar las direcciones de subred, según los siguientes requisitos:

1. Asigne la subred 0 de la red 100.10.0.0/8 al enlace entre R1 y R4.
2. Asigne la subred 1 de la red 100.10.0.0/8 al enlace entre R2 y R4.
3. Asigne la subred 2 de la red 100.10.0.0/8 al enlace entre R3 y R4.
4. Asigne la subred 3 de la red 100.10.0.0/8 al enlace entre R4 y R5.
5. Asigne la subred 4 de la red 100.10.0.0/8 al enlace entre R4 y R6.
6. Asigne la subred 5 de la red 100.10.0.0/8 al enlace entre R5 y RA.
7. Asigne la subred 0 de la red 192.168.1.0/24 a la LAN R1.
8. Asigne la subred 1 de la red 192.168.1.0/24 a la LAN R2.
9. Asigne la subred 2 de la red 192.168.1.0/24 a la LAN R4.
10. Asigne la subred 3 de la red 192.168.1.0/24 a la LAN RA.

Red: 100.10.0.0/8	
Enlace entre:	N° Subred
R1-R4	Subred 0 :
R2-R4	Subred 1 :
R3-R4	Subred 2 :
R4-R5	Subred 3 :
R4-R6	Subred 4 :
R5-RA	Subred 5 :

Tabla 5.1.2 Asignación de subredes

Red: 192.168.1.0/24	
LAN	N° Subred
R1	Subred 0 :
R2	Subred 1 :
R4	Subred 2 :
RA	Subred 3 :

Tabla 5.1.3 Asignación de subredes

PASO 2: Responder las siguientes preguntas.

1. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R1?

_____

2. ¿Qué mascara de subred utilizará la subred LAN de R1?

_____

3. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R2?

_____

4. ¿Qué mascara de subred utilizará la subred LAN de R2?

_____

5. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R4?

_____

6. ¿Qué mascara de subred utilizará la subred LAN de R4?

_____

7. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de RA?

_____

8. ¿Qué mascara de subred utilizará la subred LAN de RA?

_____

9. ¿Cuántas subredes es necesario crear de la red 192.168.1.0/24?

_____

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET Y GIGABITETHERNET.

TAREA 4: CONFIGURAR LAS RUTAS ESTÁTICAS MEDIANTE UNA DIRECCIÓN DE SIGUIENTE SALTO O POR MEDIO DE UNA INTERFAZ DE SALIDA.

TAREA 5: CONFIGURAR LOS EQUIPOS DE HOST.

TAREA 6: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

TAREA 7: ANALIS DEL TRAFICO DE PAQUETES

DESAFIO 5.2: CONFIGURACION BASICA DE RIPv1

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet y GigabitEhernet.
- Configurar una ruta dinámica con el protocolo de enrutamiento RIP v1 en todos los routers.
- Verificar el enrutamiento RIP con los comandos **show** y **debug**.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

DIAGRAMA DE TOPOLOGIA

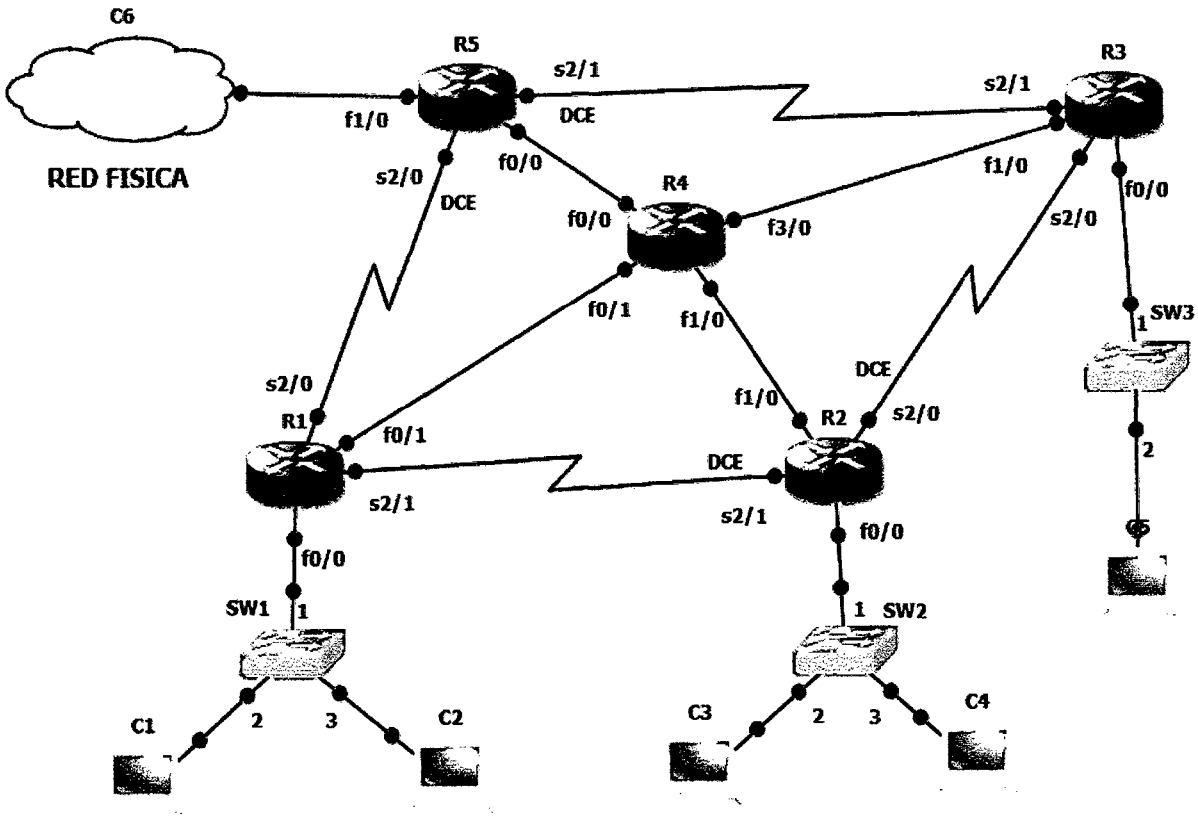


Fig. 5.2.1 Red virtual en GNS3.

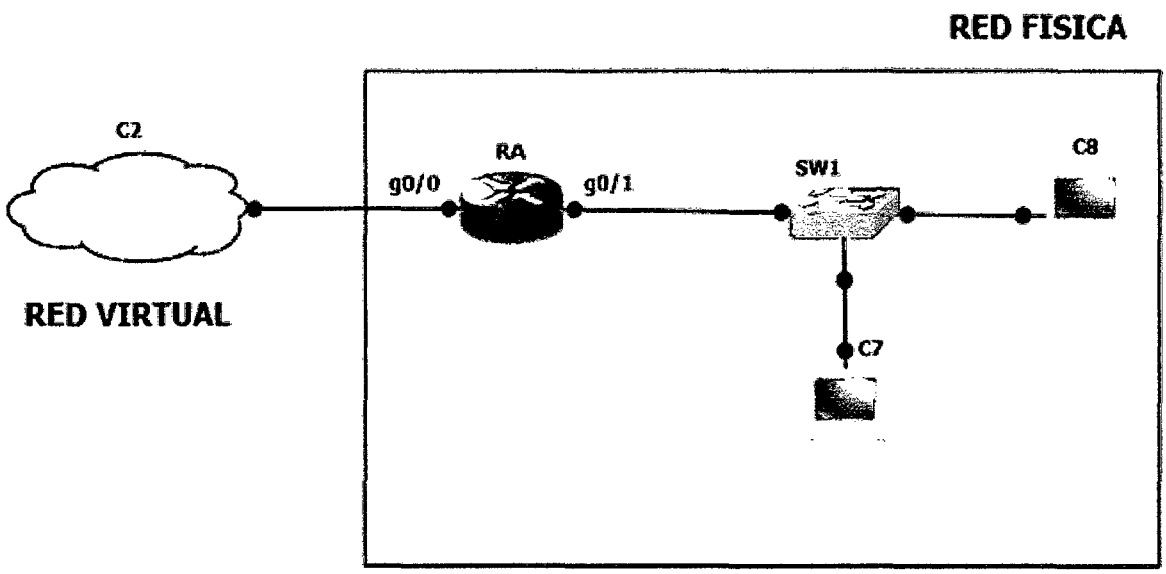


Fig. 5.2.2 Red Física.

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s2/0			
	s2/1			
	f0/0			
	f0/1			
R2	s2/0			
	s2/1			
	f1/0			
R3	s2/0			
	s2/1			
	f0/0			
	f1/0			
R4	f0/0			
	f0/1			
	f1/0			
	f3/0			
R5	s2/0			
	s2/0			
	f0/0			
	f1/0			
RA	g0/0			
	g0/1			
C1	BUCLE INVERTIDO			
C2	VPCS			
C3	VPCS			
C4	VPCS			
C5	VPCS			
C7	NIC			
C8	NIC			

Tabla 5.2.1 Tabla de direccionamiento IP para las redes.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **172.16.0.0/16** para obtener el direccionamiento IP para las conexiones entre routers, además utilice la red **192.168.0.0/22** para proporcionar direcciones para las 4 LAN:

- LAN R1: 200 host.
- LAN R2: 220 host.
- LAN R3: 100 host.
- LAN Router físico: 150 host.

PASO 1: Asignar las direcciones de subred, según los siguientes requisitos:

11. Asigne la subred 0 de la red 172.16.0.0/16 al enlace entre R5 y R3.
12. Asigne la subred 1 de la red 172.16.0.0/16 al enlace entre R5 y R1.
13. Asigne la subred 2 de la red 172.16.0.0/16 al enlace entre R5 y R4.
14. Asigne la subred 3 de la red 172.16.0.0/16 al enlace entre R3 y R2.
15. Asigne la subred 4 de la red 172.16.0.0/16 al enlace entre R4 y R1.
16. Asigne la subred 5 de la red 172.16.0.0/16 al enlace entre R4 y R2.
17. Asigne la subred 6 de la red 172.16.0.0/16 al enlace entre R1 y R2.
18. Asigne la subred 7 de la red 172.16.0.0/16 al enlace entre R5 y RA.
19. Asigne la subred 0 de la red 192.168.0.0/22 a la LAN R1.
20. Asigne la subred 1 de la red 192.168.0.0/22 a la LAN R2.
21. Asigne la subred 2 de la red 192.168.0.0/22 a la LAN R3.
22. Asigne la subred 3 de la red 192.168.0.0/22 a la LAN RA.

Red: 172.16.0.0/16	
Enlace entre:	N° Subred
R5-R3	Subred 0 :
R5-R1	Subred 1 :
R5-R4	Subred 2 :
R3-R2	Subred 3 :
R4-R1	Subred 4 :
R4-R2	Subred 5 :
R1-R2	Subred 6 :
R5-RA	Subred 7 :

Tabla 5.2.2 Tabla de subredes designadas a enlaces WAN.

Red: 192.168.0.0/22	
LAN	N° Subred
R1	Subred 0 :
R2	Subred 1 :
R3	Subred 2 :
RA	Subred 3 :

Tabla 5.2.3 Tabla de subredes designadas a enlaces LAN.

PASO 2: Responder las siguientes preguntas.

1. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R1?

_____

2. ¿Qué mascara de subred utilizará la subred LAN de R1?

_____

3. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R2?

_____

4. ¿Qué mascara de subred utilizará la subred LAN de R2?

_____

5. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R4?

_____

6. ¿Qué mascara de subred utilizará la subred LAN de R3?

_____

7. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de RA?

_____

8. ¿Qué mascara de subred utilizará la subred LAN de RA?

_____

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET Y GIGABITETHERNET.

TAREA 4: CONFIGURAR LAS RUTAS DINÁMICAS MEDIANTE EL PROTOCOLO DE ENRRUTAMIENTO RIPv1.

TAREA 5: CONFIGURAR LOS EQUIPOS DE HOST.

TAREA 6: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

TAREA 7: ANALIS DEL TRAFICO DE PAQUETES.

DESAFIO 5.3: CONFIGURACION BASICA DE RIPv2

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Determinar la cantidad de subredes necesarias.
- Determinar la cantidad de hosts necesarios para cada subred.
- Diseñar un esquema de direccionamiento adecuado utilizando VLSM.
- Asignar direcciones y pares de máscaras de subred a las interfaces del dispositivo.
- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet y GigabitEhernet.
- Configurar una ruta dinámica con el protocolo de enrutamiento RIP v2 en todos los routers.
- Verificar el enrutamiento RIPv2 con los comandos **show ip route, show ip protocols** y las actualizaciones de enrutamiento con **debug ip rip**.
- Desactive la sumarización automática.
- Examinar las tablas de enrutamiento.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

DIAGRAMA DE TOPOLOGIA

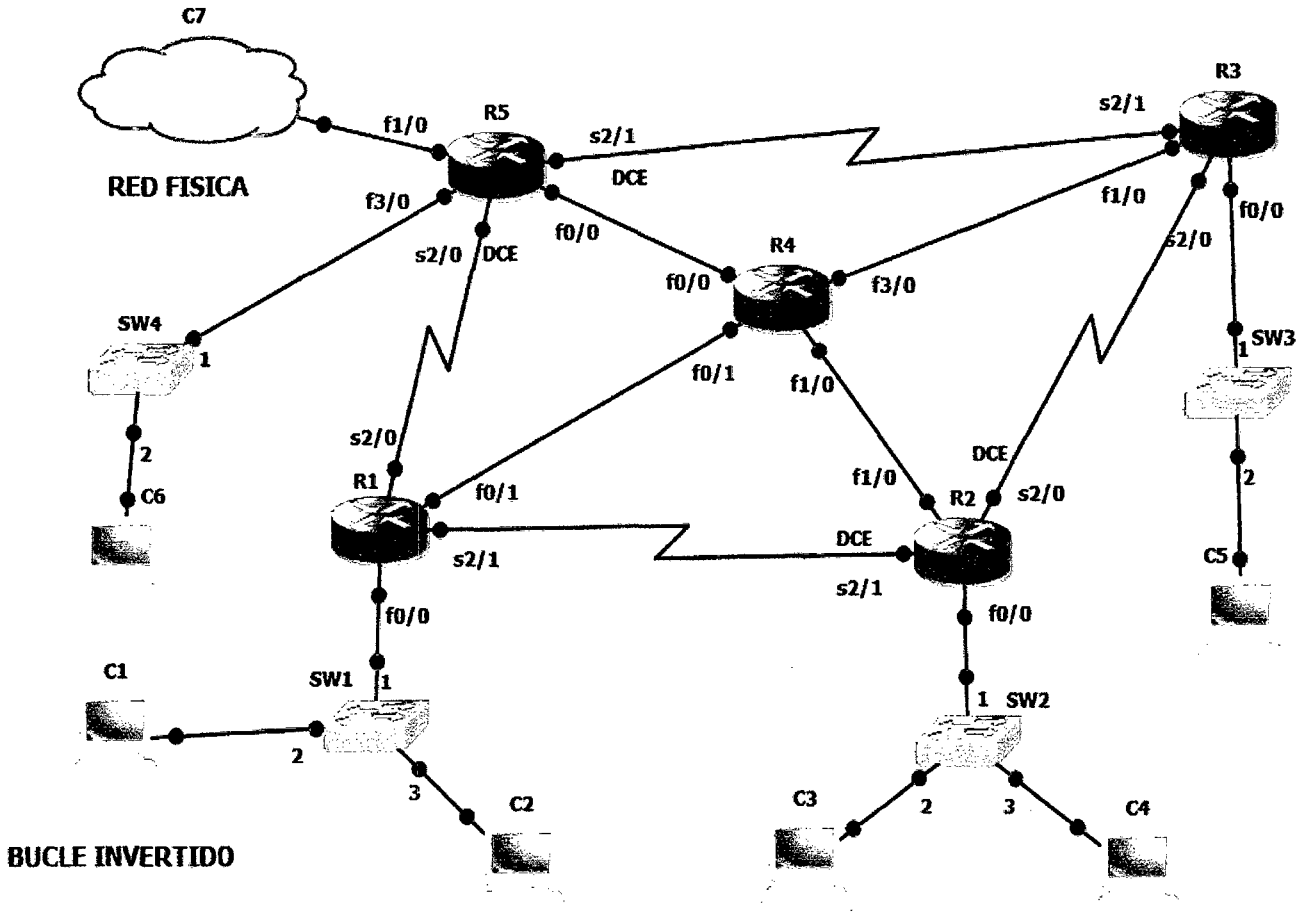


Fig. 5.3.1 Red virtual en GNS3.

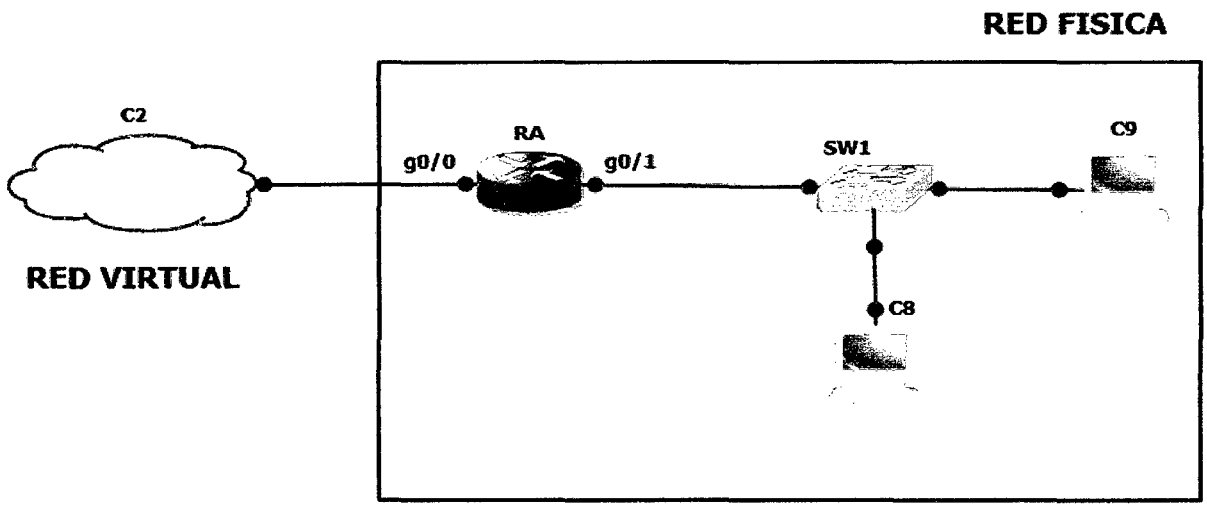


Fig. 5.3.2 Red Física.

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s2/0			
	s2/1			
	f0/0			
	f0/1			
R2	s2/0			
	s2/1			
	f1/0			
R3	s2/0			
	s2/1			
	f0/0			
	f1/0			
R4	f0/0			
	f0/1			
	f1/0			
	f3/0			
R5	s2/0			
	s2/0			
	f0/0			
	f1/0			
RA	g0/0			
	g0/1			
C1	BUCLE INVERTIDO			
C2	VPCS			
C3	VPCS			
C4	VPCS			
C5	VPCS			
C6	VPCS			
C8	NIC			
C9	NIC			

Tabla 5.3.1 Tabla de direccionamiento IP para las redes.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **172.16.0.0/16** para obtener el direccionamiento IP para las conexiones entre routers, y también para proporcionar direcciones para las 5 LAN:

- LAN R1: 100 host.
- LAN R2: 50 host.
- LAN R3: 80 host.
- LAN R5: 20 host.
- LAN Router físico: 220 host.

PASO 1: Asignar las direcciones de subred, según los siguientes requisitos:

23. Asigne la subred 0 de la red 172.16.0.0/16 al enlace entre R5 y R3.
24. Asigne la subred 1 de la red 172.16.0.0/16 al enlace entre R5 y R1.
25. Asigne la subred 2 de la red 172.16.0.0/16 al enlace entre R5 y R4.
26. Asigne la subred 3 de la red 172.16.0.0/16 al enlace entre R3 y R2.
27. Asigne la subred 4 de la red 172.16.0.0/16 al enlace entre R4 y R1.
28. Asigne la subred 5 de la red 172.16.0.0/16 al enlace entre R4 y R2.
29. Asigne la subred 6 de la red 172.16.0.0/16 al enlace entre R1 y R2.
30. Asigne la subred 7 de la red 172.16.0.0/16 al enlace entre R5 y RA.
31. Asigne la subred 0 de la red 172.16.0.0/16 a la LAN R1.
32. Asigne la subred 1 de la red 172.16.0.0/16 a la LAN R2.
33. Asigne la subred 2 de la red 172.16.0.0/16 a la LAN R3.
34. Asigne la subred 3 de la red 172.16.0.0/16 a la LAN R5.
35. Asigne la subred 4 de la red 172.16.0.0/16 a la LAN RA.

Red: 172.16.0.0/16	
Enlace entre:	N° Subred
R5-R3	Subred 0 :
R5-R1	Subred 1 :
R5R4	Subred 2 :
R3-R2	Subred 3 :
R4-R1	Subred 4 :
R4-R2	Subred 5 :
R1-R2	Subred 6 :
R5-RA	Subred 7 :

Tabla 5.3.2 Tabla de subredes designadas a enlaces WAN.

Red: 172.16.0.0/16	
LAN	N° Subred
R1	Subred 0 :
R2	Subred 1 :
R3	Subred 2 :
R5	Subred 3:
RA	Subred 4 :

Tabla 5.3.3 Tabla de subredes designadas a enlaces LAN.

PASO 2: Responder las siguientes preguntas.

1. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R1?

---

2. ¿Qué mascara de subred utilizará la subred LAN de R1?

---

3. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R2?

---

4. ¿Qué mascara de subred utilizará la subred LAN de R2?

---

5. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R3?

---

6. ¿Qué mascara de subred utilizará la subred LAN de R3?

---

7. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R5?

---

8. ¿Qué mascara de subred utilizará la subred LAN de R5?

---

9. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de RA?

10. ¿Qué mascara de subred utilizará la subred LAN de RA?

11. ¿Cuántas subredes es necesario crear de la red 172.16.0.0/16?

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET Y GIGABITETHERNET.

TAREA 4: CONFIGURAR LAS RUTAS DINÁMICAS MEDIANTE EL PROTOCOLO DE ENRRUTAMIENTO RIPv2.

TAREA 5: CONFIGURAR LOS EQUIPOS DE HOST.

TAREA 6: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

TAREA 7: ANALIS DEL TRAFICO DE PAQUETES.

DESAFIO 5.4: CONFIGURACION EIGRP

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet y GigabitEhernet.
- Configurar el enrutamiento EIGRP.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

DIAGRAMA DE TOPOLOGIA

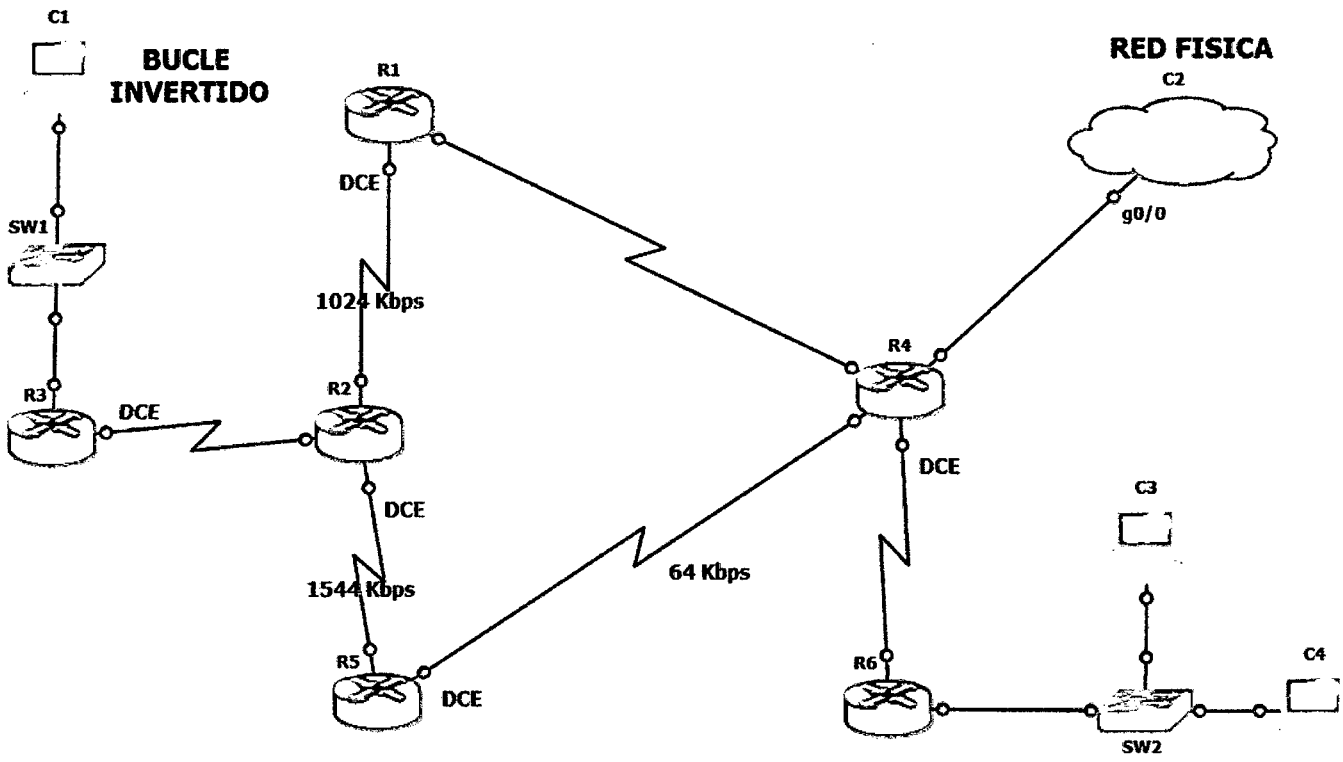


Fig. 5.4.1 Red Virtual en GNS3.

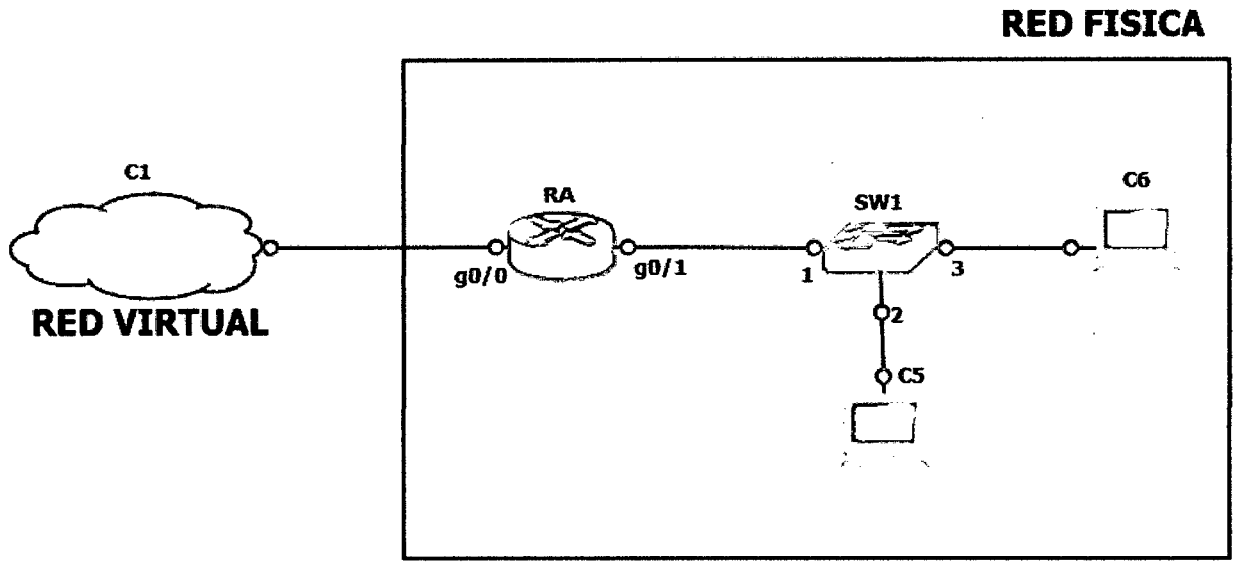


Fig. 5.4.2 Red Física.

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s0/0			
	s0/1			
R2	s0/0			
	s0/1			
	s0/2			
R3	s0/0			
	f1/0			
R4	s0/0			
	s0/1			
	s0/2			
	f1/0			
R5	s0/0			
	s0/1			
R6	s0/0			
	f1/0			
RA	g0/0			
	g0/1			
C1	BUCLE INVERTIDO			
C3	VPCS			
C4	VPCS			
C5	NIC			
C6	NIC			

Tabla 5.4.1 Direccionamiento IP para las Redes

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Configurar sistema autónomo 10, la red **80.0.0.0/8** debe dividirse en subredes para obtener direccionamiento IP usando VLSM para los enlaces entre routers, además dividir la red **170.0.0.0/16** para proporcionar direcciones para las 3 LAN:

- LAN de R3 necesitara 200 direcciones.
- LAN de R6 necesitara 150 direcciones.
- LAN de RA necesitara 100 direcciones.

PASO 1: Asignar las direcciones de subred, según los siguientes requisitos:

36. Asigne la subred 0 de la red 80.0.0.0/8 al enlace entre R1 y R2.
37. Asigne la subred 1 de la red 80.0.0.0/8 al enlace entre R1 y R4.
38. Asigne la subred 2 de la red 80.0.0.0/8 al enlace entre R2 y R3.
39. Asigne la subred 3 de la red 80.0.0.0/8 al enlace entre R2 y R5.
40. Asigne la subred 4 de la red 80.0.0.0/8 al enlace entre R4 y R5.
41. Asigne la subred 5 de la red 80.0.0.0/8 al enlace entre R4 y R6.
42. Asigne la subred 6 de la red 80.0.0.0/8 al enlace entre R4 y RA.
43. Asigne la subred 0 de la red 170.0.0.0/16 a la LAN R3.
44. Asigne la subred 1 de la red 170.0.0.0/16 a la LAN R6.
45. Asigne la subred 2 de la red 170.0.0.0/16 a la LAN RA.

Red: 10.0.0.0/8	
Enlace entre:	N° Subred
R1-R2	Subred 0 :
R1-R4	Subred 1 :
R2-R3	Subred 2 :
R2-R5	Subred 3 :
R4-R5	Subred 4 :
R4-R6	Subred 5 :
R4-RA	Subred 6 :

Tabla 5.4.2 Asignación de subredes

Red: 170.0.0.0/16	
LAN	N° Subred
R3	Subred 0 :
R6	Subred 1 :
RA	Subred 2 :

Tabla 5.4.3 Asignación de subredes

PASO 2: Responder las siguientes preguntas.

1. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R3?

---

2. ¿Qué mascara de subred utilizará la subred LAN de R3?

---

3. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R6?

---

4. ¿Qué mascara de subred utilizará la subred LAN de R6?

---

5. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de RA?

---

6. ¿Qué mascara de subred utilizará la subred LAN de RA?

---

7. ¿Cuántas subredes es necesario crear de la red 170.0.0.0/16?

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET Y GIGABITETHERNET.

TAREA 4: CONFIGURAR EIGRP.

TAREA 5: CONFIGURAR LOS EQUIPOS DE HOST.

TAREA 6: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

TAREA 7: ANALIS DEL TRAFICO DE PAQUETES

DESAFIO 5.5: CONFIGURACION OSPF

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet y GigabitEhernet.
- Configurar el enrutamiento OSPF.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

DIAGRAMA DE TOPOLOGIA

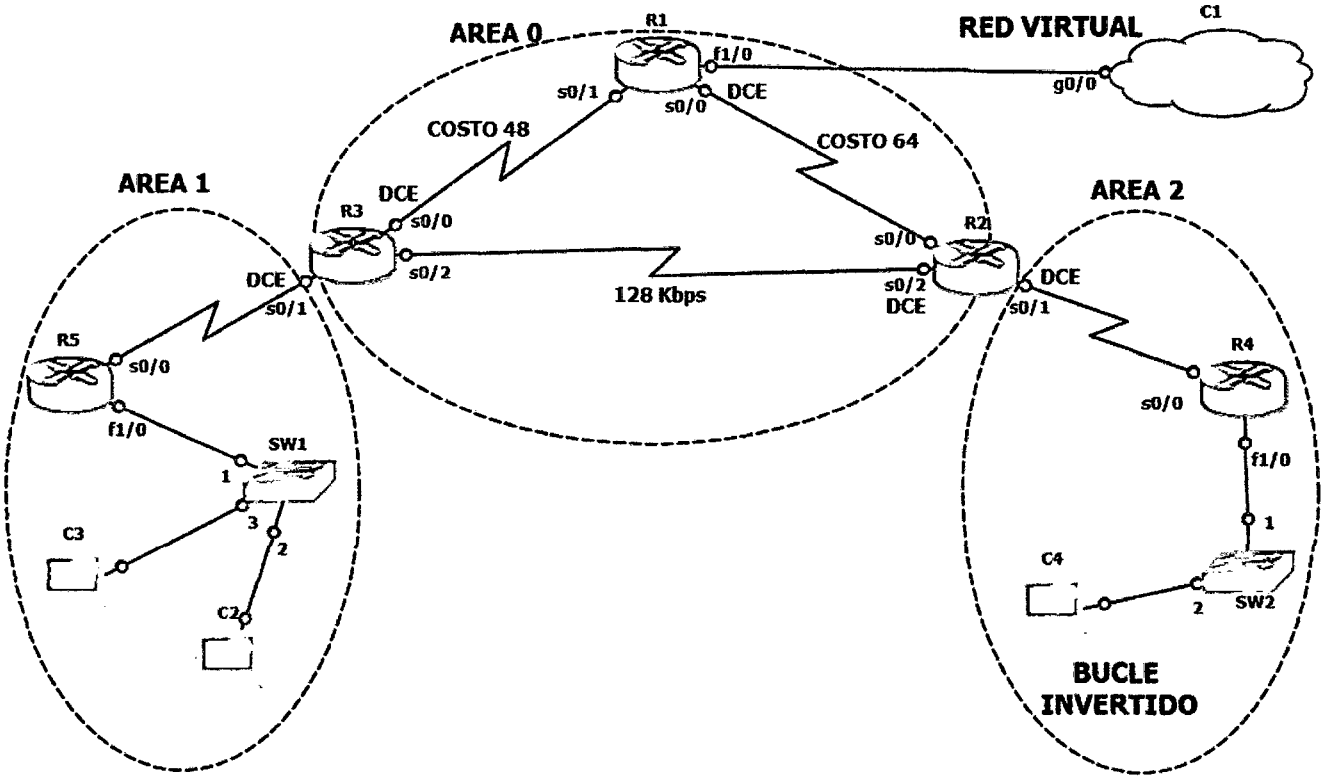


Fig. 5.5.1 Red Virtual en GNS3

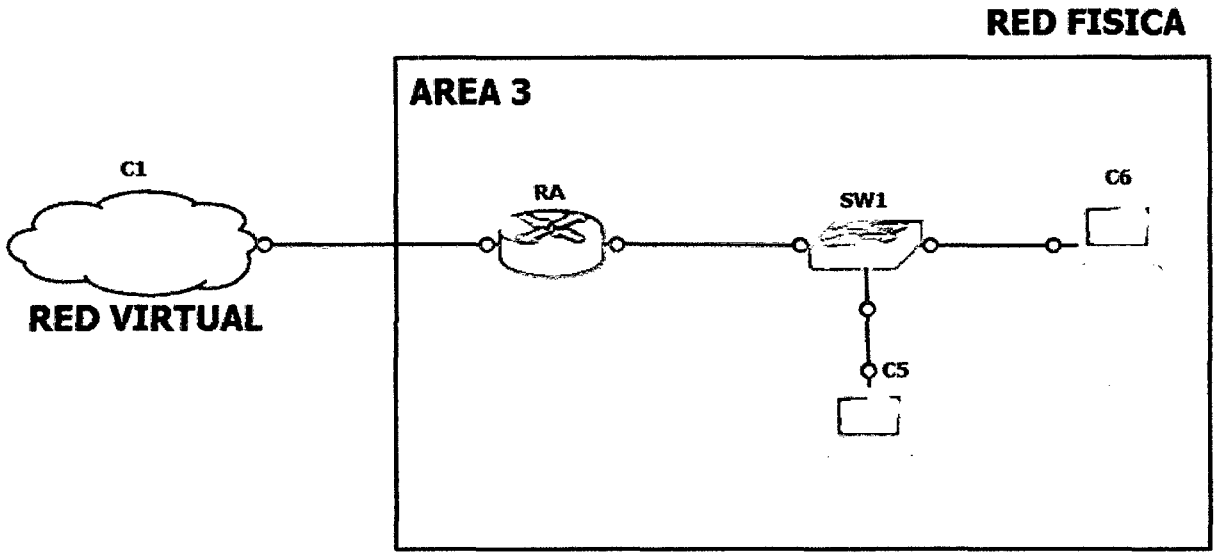


Fig. 5.5.2 Red Física

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s0/0			
	s0/1			
	s0/2			
	f1/0			
R2	s0/0			
	s0/1			
	s0/2			
R3	s0/0			
	s0/1			
	s0/2			
R4	s0/0			
	f1/0			
R5	s0/0			
	f1/0			
RA	g0/0			
	g0/1			
C2	VPCS			
C3	VPCS			
C4	BUCLE INVERTIDO			
C5	NIC			
C6	NIC			

Tabla 5.5.1 Direccionamiento IP para las Redes

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Configurar ID de proceso 100 en todos los routers, la red **20.0.0.0/8** debe dividirse en subredes para obtener direccionamiento IP usando VLSM para los enlaces entre routers, además dividir la red **140.0.0.0/16** para proporcionar direcciones para las 3 LAN:

- LAN de R4 necesitara 1500 direcciones.
- LAN de R5 necesitara 800 direcciones.
- LAN de RA necesitara 600 direcciones.

PASO 1: Asignar las direcciones de subred, según los siguientes requisitos:

46. Asigne la subred 0 de la red 20.0.0.0/8 al enlace entre R1 y RA.
47. Asigne la subred 1 de la red 20.0.0.0/8 al enlace entre R1 y R2.
48. Asigne la subred 2 de la red 20.0.0.0/8 al enlace entre R1 y R3.
49. Asigne la subred 3 de la red 20.0.0.0/8 al enlace entre R2 y R4.
50. Asigne la subred 4 de la red 20.0.0.0/8 al enlace entre R3 y R5.
51. Asigne la subred 0 de la red 140.0.0.0/16 a la LAN RA.
52. Asigne la subred 1 de la red 140.0.0.0/16 a la LAN R4.
53. Asigne la subred 2 de la red 140.0.0.0/16 a la LAN R5.

Red: 20.0.0.0/8	
Enlace entre:	N° Subred
R1-RA	Subred 0 :
R1-R2	Subred 1 :
R1-R3	Subred 2 :
R2-R4	Subred 3 :
R3-R5	Subred 4 :

Tabla 5.5.2 Asignación de subredes

Red: 140.0.0.0/16	
LAN	N° Subred
R3	Subred 0 :
R6	Subred 1 :
RA	Subred 2 :

Tabla 5.5.3 Asignación de subredes

PASO 2: Responder las siguientes preguntas.

1. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de RA?

---

2. ¿Qué mascara de subred utilizará la subred LAN de RA?

---

3. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R4?

---

4. ¿Qué mascara de subred utilizará la subred LAN de R4?

---

5. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R5?

---

6. ¿Qué mascara de subred utilizará la subred LAN de R5?

---

7. ¿Cuántas subredes es necesario crear de la red 140.0.0.0/16?

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET Y GIGABITETHERNET.

TAREA 4: CONFIGURAR ENRUTAMIENTO OSPF.

PASO 1: Al configurar OSPF declar el ID de proceso y las redes directamente conectadas.

PASO 2: Modificar bandwidth.

PASO 3: Modificar el costo del enlace.

TAREA 5: CONFIGURAR LOS EQUIPOS DE HOST.

TAREA 6: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

TAREA 7: *ANALIS DEL TRAFICO DE PAQUETES.*

DESAFIO 5.6: CONFIGURACION BASICA DE BGP

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar interfaces.
- Configurar el enrutamiento BGP externo (eBGP) en los routers de borde.
- Configurar el enrutamiento BGP interno (iBGP) en los routers del mismo AS.
- Configurar el enrutamiento OSPF en todos los routers conforme su AS.
- Configurar las ID del router OSPF.
- Verificar el enrutamiento OSPF por medio de los comandos show.
- Verificar el enrutamiento BGP por medio de los comandos show.
- Probar la conectividad en la red.
- Análisis de tráfico de paquetes.

DIAGRAMA DE TOPOLOGIA

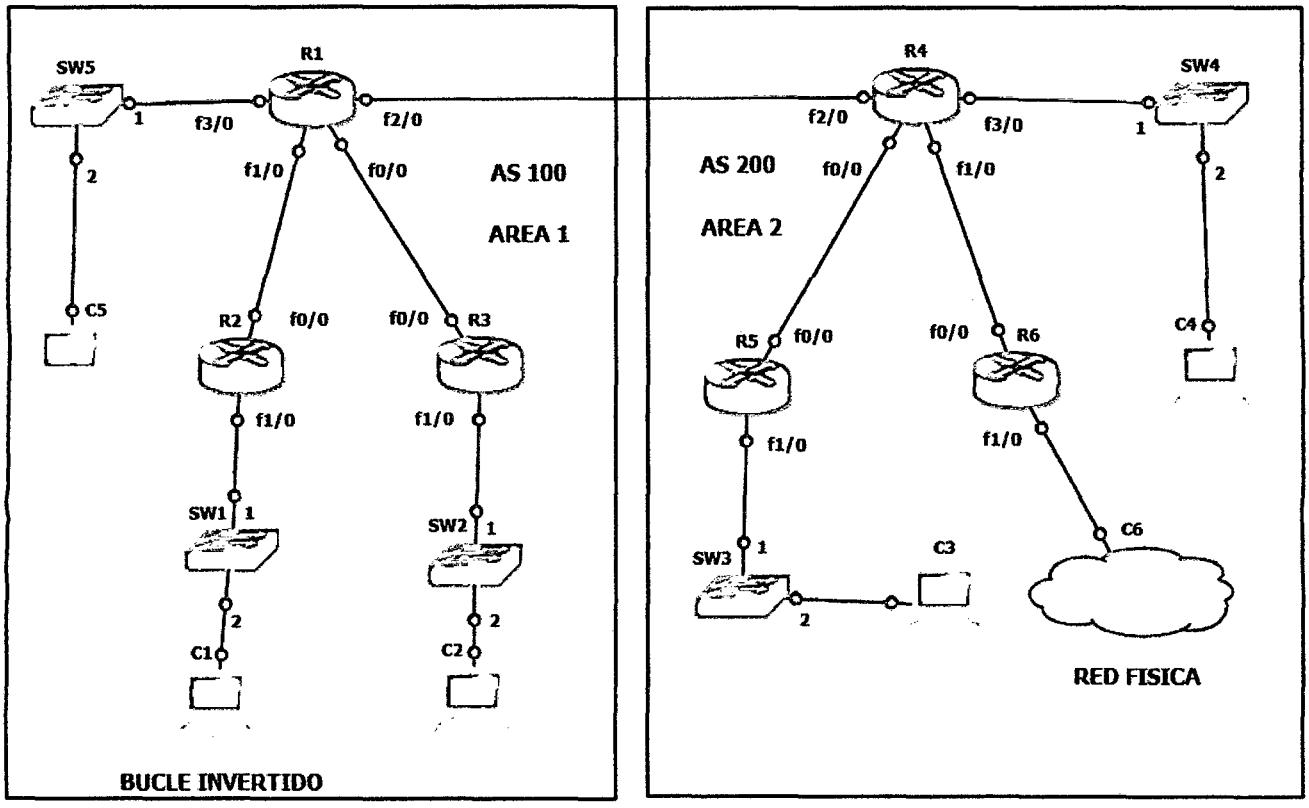


Fig. 5.6.1 Red virtual en GNS3.

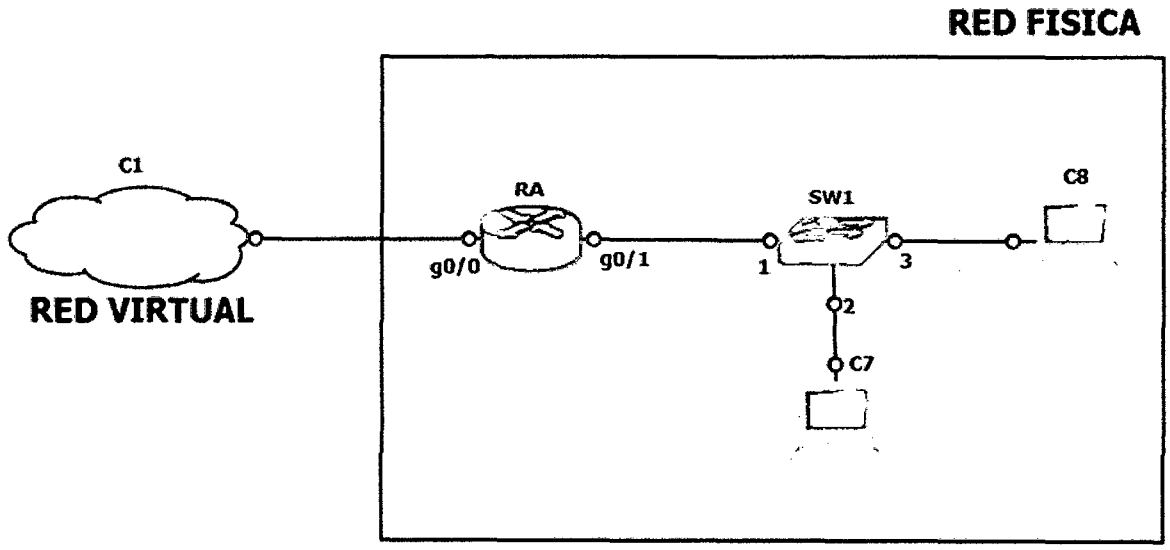


Fig. 5.6.2 Red Física.

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	f0/0			
	f1/0			
	f2/0			
	f3/0			
R2	f0/0			
	f1/0			
R3	f0/0			
	f1/0			
R4	f0/0			
	f1/0			
	f2/0			
	f3/0			
R5	f0/0			
	f1/0			
R6	f0/0			
	f1/0			
RA	g0/0			
	g0/1			
C1	BUCLE INVERTIDO			
C2	VPCS			
C3	VPCS			
C4	VPCS			
C5	VPCS			
C7	NIC			
C8	NIC			

Tabla 5.6.1 Tabla de direccionamiento IP para las redes.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **150.150.0.0/16** para obtener el direccionamiento IP para las conexiones entre routers, y también para proporcionar direcciones para las 6 LAN:

- LAN R1: 120 host.
- LAN R2: 90 host.
- LAN R3: 80 host.
- LAN R4: 50
- LAN R5: 50 host.
- LAN Router físico: 200 host.

PASO 1: Asignar las direcciones de subred, según los siguientes requisitos:

54. Asigne la subred 0 de la red 150.150.0.0/16 al enlace entre R1 y R2.
55. Asigne la subred 1 de la red 150.150.0.0/16 al enlace entre R1 y R3.
56. Asigne la subred 2 de la red 150.150.0.0/16 al enlace entre R1 y R4.
57. Asigne la subred 3 de la red 150.150.0.0/16 al enlace entre R4 y R5.
58. Asigne la subred 4 de la red 150.150.0.0/16 al enlace entre R4 y R6.
59. Asigne la subred 5 de la red 150.150.0.0/16 al enlace entre R6 y RA.
60. Asigne la subred 0 de la red 150.150.0.0/16 a la LAN R1.
61. Asigne la subred 1 de la red 150.150.0.0/16 a la LAN R2.
62. Asigne la subred 2 de la red 150.150.0.0/16 a la LAN R3.
63. Asigne la subred 3 de la red 150.150.0.0/16 a la LAN R4.
64. Asigne la subred 4 de la red 150.150.0.0/16 a la LAN R5.
65. Asigne la subred 5 de la red 150.150.0.0/16 a la LAN RA.

Red: 150.150.0.0/16	
Enlace entre:	N° Subred
R1-R2	Subred 0 :
R1-R3	Subred 1 :
R1-R4	Subred 2 :
R4-R5	Subred 3 :
R4-R6	Subred 4 :
R6-RA	Subred 5 :

Tabla 5.6.2 Asignación de subredes.

Red: 150.150.0.0/16	
LAN	N° Subred
R1	Subred 0 :
R2	Subred 1 :
R3	Subred 2 :
R4	Subred 3 :
R5	Subred 4 :
RA	Subred 5 :

Tabla 5.6.3 Asignación de subredes.

PASO 2: Responder las siguientes preguntas.

1. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R1?

_____

2. ¿Qué mascara de subred utilizará la subred LAN de R1?

_____

3. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R2?

_____

4. ¿Qué mascara de subred utilizará la subred LAN de R2?

_____

5. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R3?

_____

6. ¿Qué mascara de subred utilizará la subred LAN de R3?

_____

7. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R4?

_____

8. ¿Qué mascara de subred utilizará la subred LAN de R4?

9. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R5?

10. ¿Qué mascara de subred utilizará la subred LAN de R5?

11. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de RA?

12. ¿Qué mascara de subred utilizará la subred LAN de RA?

13. ¿Cuántas subredes es necesario crear de la red 150.150.0.0/16?

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET Y GIGABITETHERNET.

TAREA 4: CONFIGURAR EL PROTOCOLO DE ENRUTAMIENTO OSPF EN LOS ROUTERS.

TAREA 5: CONFIGURAR EL PROTOCOLO DE ENRUTAMIENTO BGP EN LOS ROUTERS.

TAREA 6: CONFIGURAR LOS EQUIPOS DE HOST.

TAREA 7: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

TAREA 8: ANALIS DEL TRAFICO DE PAQUETES.

DESAFIO 5.7: CONFIGURACIÓN BASICA DE ENRUTAMIENTO INTER VLAN

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología.
- Borrar las configuraciones y volver a cargar un switch y un router al estado predeterminado.
- Realizar las tareas básicas de configuración en una LAN conmutada y un router.
- Configurar las VLAN y el protocolo VLAN Trunking (VTP) en todos los switches.
- Configurar un router para admitir el enlace 802.1q en una interfaz Fast Ethernet.
- Configurar un router con subinterfaces que correspondan a las VLAN configuradas.
- Configurar un router con el protocolo de enrutamiento OSPF.
- Demostrar y explicar el enrutamiento entre VLAN.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

DIAGRAMA DE TOPOLOGIA

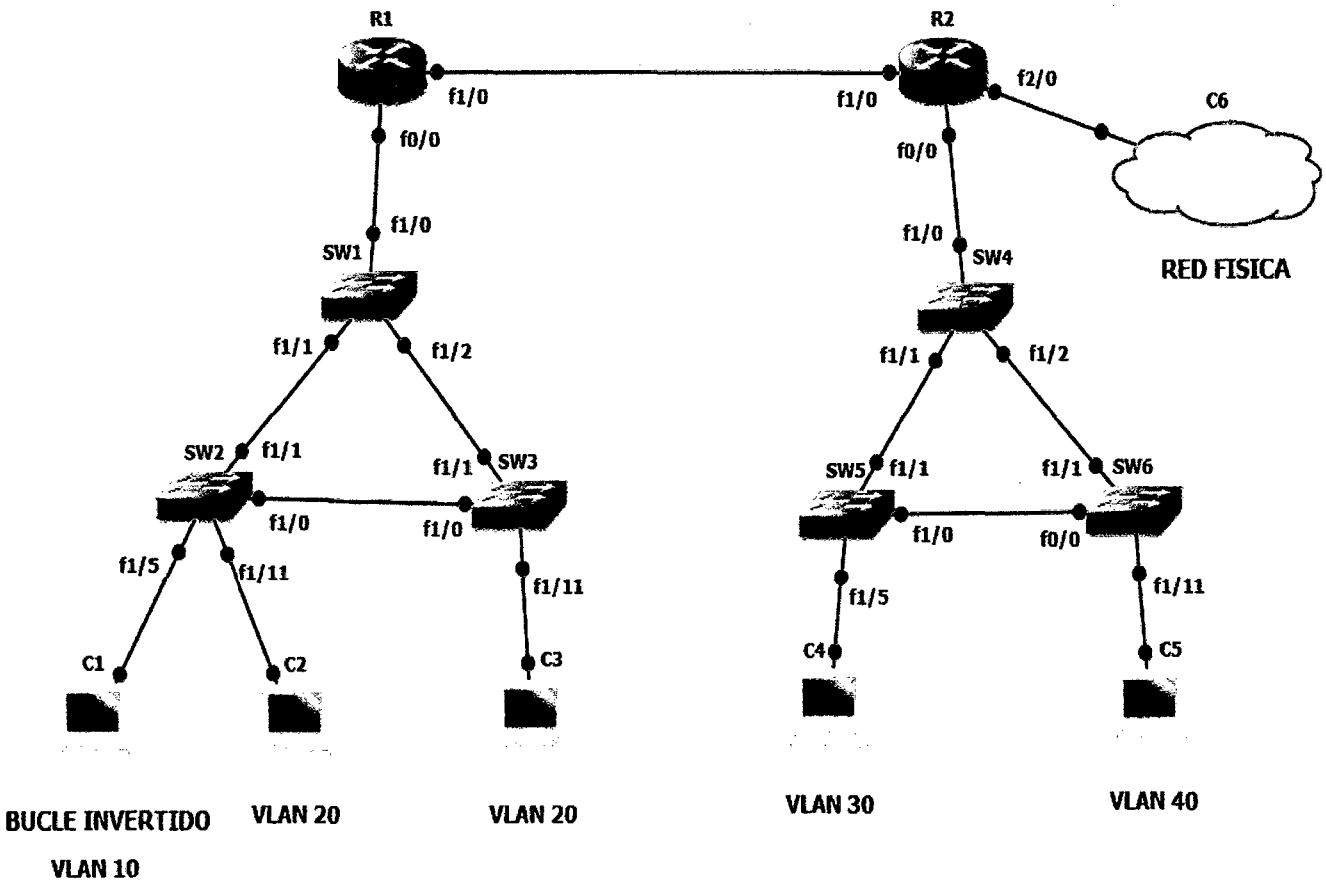


Fig. 5.7.1 Red virtual en GNS3.

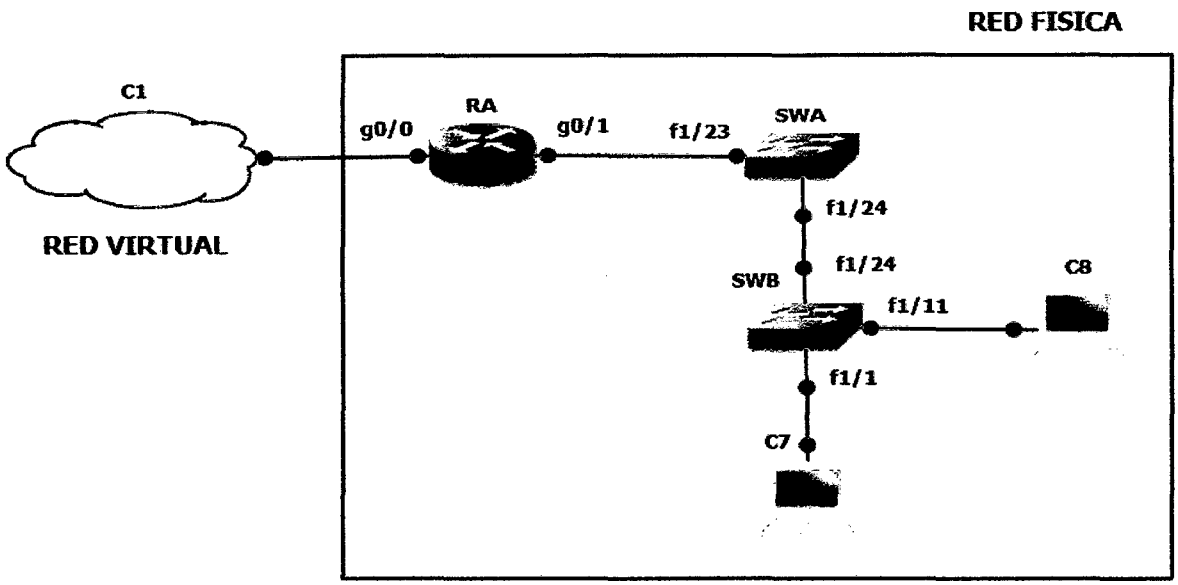


Fig. 5.7.2 Red Física.

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	f1/0			
	f0/0.1			
	f0/0.10			
	f0/0.20			
R2	f0/0			
	f0/1.30			
	f0/1.40			
	f0/1.1			
RA	g0/0			
	g0/1.50			
	g0/1.50			
	g0/1.1			
C1	BUCLE INVERTIDO			
C2	VPCS			
C3	VPCS			
C4	VPCS			
C5	VPCS			
C7	NIC			
C8	NIC			

Tabla 5.7.1 Tabla de direccionamiento IP para las redes.

ASIGNACIONES DE PUERTO: SW1

Puertos	Asignación	Red
f 1/0 – f 1/2	Enlaces troncales 802.1q (LAN 1 nativa)	

Tabla 5.7.2 Asignación de Puertos SW1.

ASIGNACIONES DE PUERTO: SW2

Puertos	Asignación	Red
f1/0 – f1/1	Enlaces troncales 802.1q (LAN 1 nativa)	
f1/5 – f1/10	Vlan 10	
f1/11 – f1/15	Vlan 20	

Tabla 5.7.3 Asignación de Puertos SW2.

ASIGNACIONES DE PUERTO: SW3

Puertos	Asignación	Red
f1/0 – f1/1	Enlaces troncales 802.1q (LAN 1 nativa)	
f1/5 – f1/10	Vlan 10	
f1/11 – f1/15	Vlan 20	

Tabla 5.7.4 Asignación de Puertos SW3.

ASIGNACIONES DE PUERTO: SW4

Puertos	Asignación	Red
f1/0 – f1/2	Enlaces troncales 802.1q (LAN 99 nativa)	

Tabla 5.7.5 Asignación de Puertos SW4.

ASIGNACIONES DE PUERTO: SW5

Puertos	Asignación	Red
f1/0 – f1/1	Enlaces troncales 802.1q (LAN 99 nativa)	
f1/5 – f1/10	Vlan 30	
f1/10 – f1/15	Vlan 40	

Tabla 5.7.6 Asignación de Puertos SW5.

ASIGNACIONES DE PUERTO: SW6

Puertos	Asignación	Red
f1/0 – f1/1	Enlaces troncales 802.1q (LAN 99 nativa)	
f1/5 – f1/10	Vlan 30	
f1/10 – f1/15	Vlan 40	

Tabla 5.7.7 Asignación de Puertos SW6.

ASIGNACIONES DE PUERTO: SWA

Puertos	Asignación	Red
f1/23 – f1/24	Enlaces troncales 802.1q (LAN 99 nativa)	

Tabla 5.7.8 Asignación de Puertos SWA.

ASIGNACIONES DE PUERTO: SWB

Puertos	Asignación	Red
f1/23	Enlaces troncales 802.1q (LAN 99 nativa)	
f1/1 – f1/10	Vlan 50	
f1/11 – f1/20	Vlan 60	

Tabla 5.7.9 Asignación de Puertos SWB.

Configure las siguientes VLAN en los servidores VTP:

SW1:

Vlan	Nombre de la Vlan
Vlan 10	Vlan-10
Vlan 20	Vlan-20

Tabla 5.7.10 Nombre de VLAN en SW1.

SW4:

Vlan	Nombre de la Vlan
Vlan 99	Vlan-99
Vlan 30	Vlan-30
Vlan 40	Vlan-40

Tabla 5.7.11 Nombre de VLAN en SW4.

SWA:

Vlan	Nombre de la Vlan
Vlan 99	Vlan-99
Vlan 50	Vlan-50
Vlan 60	Vlan-60

Tabla 5.7.12 Nombre de VLAN en SWA.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **172.16.0.0/16** para obtener el direccionamiento IP para las conexiones entre routers, y también para proporcionar direcciones para las 6 LAN:

- LAN VLAN 10: 200 host.
- LAN VLAN 20: 220 host.
- LAN VLAN 30: 100 host.
- LAN VLAN 40: 110 host.
- LAN VLAN 50: 220 host.
- LAN VLAN 60: 220 host.

PASO 1: Asignar las direcciones de subred, según los siguientes requisitos:

66. Asigne la subred 0 de la red 172.16.0.0/16 al enlace entre R1 y R2.
67. Asigne la subred 1 de la red 172.16.0.0/16 al enlace entre R2 y RA.
68. Asigne la subred 0 de la red 172.16.0.0/16 a la LAN VLAN 10.
69. Asigne la subred 1 de la red 172.16.0.0/16 a la LAN VLAN 20.
70. Asigne la subred 2 de la red 172.16.0.0/16 a la LAN VLAN 30.
71. Asigne la subred 3 de la red 172.16.0.0/16 a la LAN VLAN 40.
72. Asigne la subred 4 de la red 172.16.0.0/16 a la LAN VLAN 50.
73. Asigne la subred 5 de la red 172.16.0.0/16 a la LAN VLAN 60.

Red: 172.16.0.0/16	
Enlace entre:	N° Subred
R1 y R2	Subred 0 :
R2 y RA	Subred 1 :

Tabla 5.7.13 Asignación de subredes.

Red: 172.16.0.0/16	
LAN	N° Subred
VLAN 10	Subred 0 :
VLAN 20	Subred 1 :
VLAN 30	Subred 2 :
VLAN 40	Subred 3:
VLAN 50	Subred 4 :
VLAN 60	Subred 5:

Tabla 5.7.14 Asignación de subredes.

PASO 2: Responder las siguientes preguntas.

1. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de VLAN 10?

---

2. ¿Qué mascara de subred utilizará la subred LAN de VLAN 10?

---

3. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de VLAN 20?

---

4. ¿Qué mascara de subred utilizará la subred LAN de VLAN 20?

---

5. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de VLAN 30?

---

6. ¿Qué mascara de subred utilizará la subred LAN de VLAN 30?

---

7. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de VLAN 40?

---

8. ¿Qué mascara de subred utilizará la subred LAN de VLAN 40?

---

9. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de VLAN 50?

---

10. ¿Qué mascara de subred utilizará la subred LAN de VLAN 50?

---

11. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de VLAN 60?

---

12. ¿Qué mascara de subred utilizará la subred LAN de VLAN 60?

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER Y SWITCH.

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET Y GIGABITETHERNET.

TAREA 4: CONFIGURAR VTP EN LOS SWITCHES.

TAREA 5: CONFIGURAR LAS VLAN EN LOS SERVIDORES VTP.

TAREA 6: CONFIGURAR LA INTERFAZ DE ENLACES TRONCALES EN R1, R2 Y RA.

TAREA 7: CONFIGURE EL PROTOCOLO OSPF EN LOS ROUTER R1, R2 Y RA.

TAREA 8: CONFIGURE DHCP EN LOS ROUTERS R1, R2 Y RA.

TAREA 9: CONFIGURAR LOS EQUIPOS DE HOST.

TAREA 10: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

TAREA 11: ANALIS DEL TRAFICO DE PAQUETES

DESAFIO 5.8: CONFIGURACION BÁSICA DE ETHERCHANNEL

OBJETIVOS DE APRENDIZAJE

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología.
- Borrar las configuraciones y volver a cargar un switch y un router al estado predeterminado.
- Realizar las tareas básicas de configuración en una LAN conmutada y un router.
- Configurar las VLAN y el protocolo PORTCHANNEL en todos los switches.
- Configurar un router para admitir el enlace 802.1q en una interfaz Fast Ethernet.
- Configurar un router con subinterfaces que correspondan a las VLAN configuradas.
- Demostrar y explicar el enrutamiento entre VLAN.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

DIAGRAMA DE TOPOLOGIA

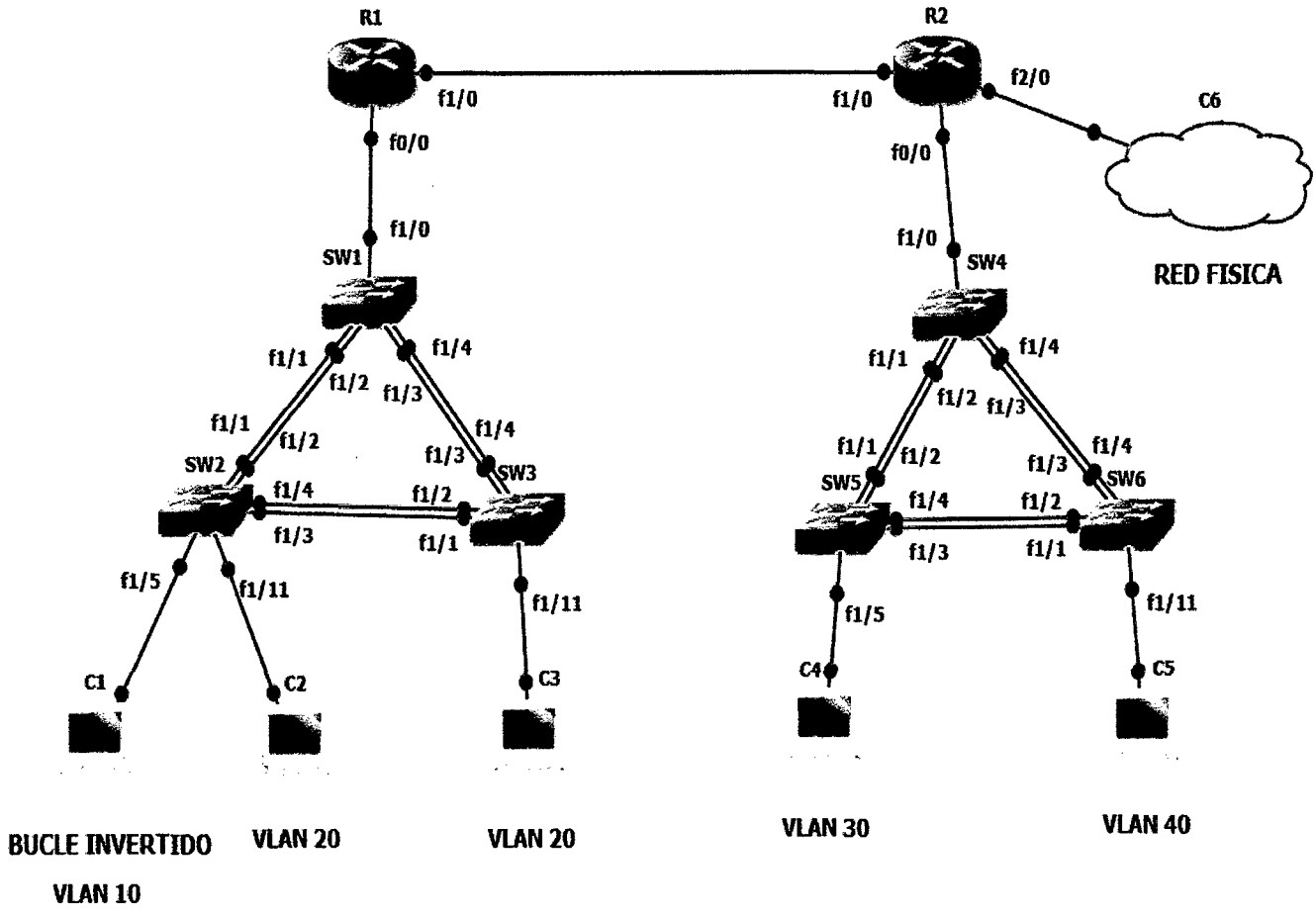


Fig. 5.8.1 Red virtual en GNS3.

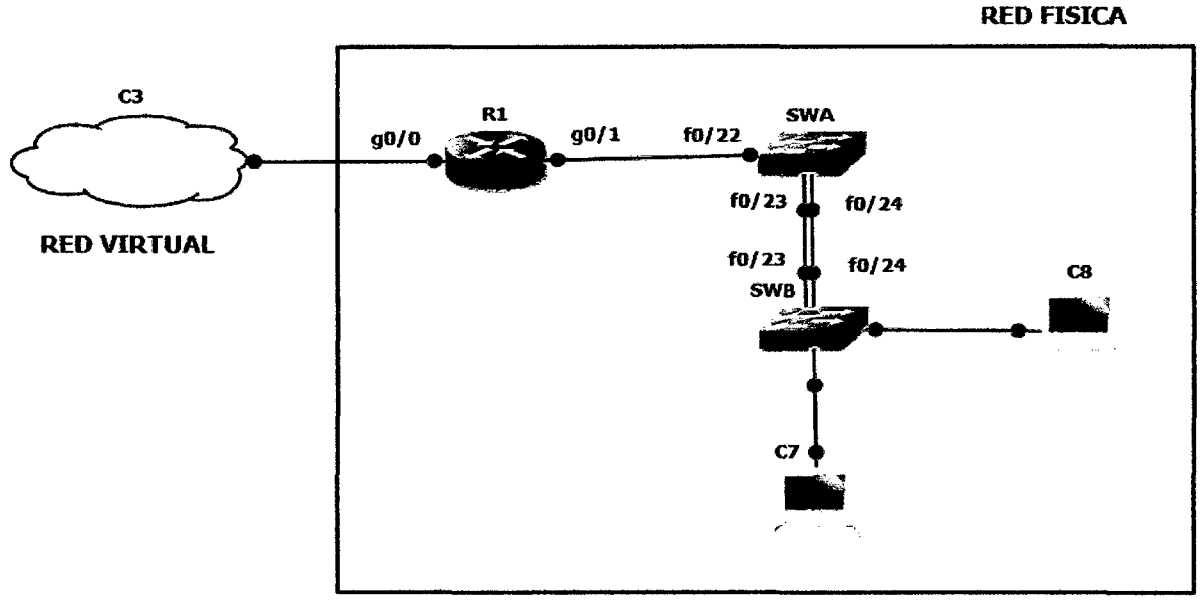


Fig. 5.8.2 Red Física.

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	f1/0			
	f0/0.1			
	f0/0.10			
	f0/0.20			
R2	f0/0			
	f0/1.30			
	f0/1.40			
	f0/1.1			
RA	g0/0			
	g0/1.50			
	g0/1.50			
	g0/1.1			
C1	BUCLE INVERTIDO			
C2	VPCS			
C3	VPCS			
C4	VPCS			
C5	VPCS			
C7	NIC			
C8	NIC			

Tabla 5.8.1 Tabla de direccionamiento IP para las redes.

ASIGNACIONES DE PUERTO: SW1

Puertos	Asignación	Red
f 1/0 – f 1/4	Enlaces troncales 802.1q (LAN 1 nativa)	

Tabla 5.8.2 Asignación de Puertos SW1.

ASIGNACIONES DE PUERTO: SW2

Puertos	Asignación	Red
f1/0 – f1/3	Enlaces troncales 802.1q (LAN 1 nativa)	
f1/5 – f1/10	Vlan 10	
f1/11 – f1/15	Vlan 20	

Tabla 5.8.3 Asignación de Puertos SW2.

ASIGNACIONES DE PUERTO: SW3

Puertos	Asignación	Red
f1/0 – f1/3	Enlaces troncales 802.1q (LAN 1 nativa)	
f1/5 – f1/10	Vlan 10	
f1/11 – f1/15	Vlan 20	

Tabla 5.8.4 Asignación de Puertos SW3.

ASIGNACIONES DE PUERTO: SW4

Puertos	Asignación	Red
f1/0 – f1/4	Enlaces troncales 802.1q (LAN 99 nativa)	

Tabla 5.8.5 Asignación de Puertos SW4.

ASIGNACIONES DE PUERTO: SW5

Puertos	Asignación	Red
f1/0 – f1/3	Enlaces troncales 802.1q (LAN 99 nativa)	
f1/5 – f1/10	Vlan 30	
f1/11 – f1/15	Vlan 40	

Tabla 5.8.6 Asignación de Puertos SW5.

ASIGNACIONES DE PUERTO: SW6

Puertos	Asignación	Red
f1/0 – f1/3	Enlaces troncales 802.1q (LAN 99 nativa)	
f1/5 – f1/10	Vlan 30	
f1/11 – f1/15	Vlan 40	

Tabla 5.8.7 Asignación de Puertos SW6.

ASIGNACIONES DE PUERTO: SWA

Puertos	Asignación	Red
f1/22 – f1/24	Enlaces troncales 802.1q (LAN 99 nativa)	

Tabla 5.8.8 Asignación de Puertos SWA.

ASIGNACIONES DE PUERTO: SWB

Puertos	Asignación	Red
f1/23 - 24	Enlaces troncales 802.1q (LAN 99 nativa)	
f1/1 – f1/10	Vlan 50	
f1/11 – f1/20	Vlan 60	

Tabla 5.8.9 Asignación de Puertos SWB.

Configure las siguientes VLAN en los servidores VTP:

SW1:

Vlan	Nombre de la Vlan
Vlan 10	Vlan-10
Vlan 20	Vlan-20

Tabla 5.8.10 Nombre de VLAN en SW1.

SW4:

Vlan	Nombre de la Vlan
Vlan 99	Vlan-99
Vlan 30	Vlan-30
Vlan 40	Vlan-40

Tabla 5.8.11 Nombre de VLAN en SW4.

SWA:

Vlan	Nombre de la Vlan
Vlan 99	Vlan-99
Vlan 50	Vlan-50
Vlan 60	Vlan-60

Tabla 5.8.12 Nombre de VLAN en SWA.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **172.18.0.0/16** para obtener el direccionamiento IP para las conexiones entre routers, y también para proporcionar direcciones para las 6 LAN:

- LAN VLAN 10: 200 host.
- LAN VLAN 20: 220 host.
- LAN VLAN 30: 100 host.
- LAN VLAN 40: 110 host.
- LAN VLAN 50: 220 host.
- LAN VLAN 60: 220 host.

PASO 1: Asignar las direcciones de subred, según los siguientes requisitos:

74. Asigne la subred 0 de la red 172.18.0.0/16 al enlace entre R1 y R2.
75. Asigne la subred 1 de la red 172.18.0.0/16 al enlace entre R2 y RA.
76. Asigne la subred 0 de la red 172.18.0.0/16 a la LAN VLAN 10.
77. Asigne la subred 1 de la red 172.18.0.0/16 a la LAN VLAN 20.
78. Asigne la subred 2 de la red 172.18.0.0/16 a la LAN VLAN 30.
79. Asigne la subred 3 de la red 172.18.0.0/16 a la LAN VLAN 40.
80. Asigne la subred 4 de la red 172.18.0.0/16 a la LAN VLAN 50.
81. Asigne la subred 5 de la red 172.18.0.0/16 a la LAN VLAN 60.

Red: 172.18.0.0/16	
Enlace entre:	N° Subred
R1 y R2	Subred 0 :
R2 y RA	Subred 1 :

Tabla 5.8.13 Asignación de subredes.

Red: 172.18.0.0/16	
LAN	N° Subred
VLAN 10	Subred 0 :
VLAN 20	Subred 1 :
VLAN 30	Subred 2 :
VLAN 40	Subred 3:
VLAN 50	Subred 4 :
VLAN 60	Subred 5:

Tabla 5.8.14 Asignación de subredes.

PASO 2: Responder las siguientes preguntas.

1. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de VLAN 10?

_____

2. ¿Qué mascara de subred utilizará la subred LAN de VLAN 10?

_____

3. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de VLAN 20?

_____

4. ¿Qué mascara de subred utilizará la subred LAN de VLAN 20?

_____

5. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de VLAN 30?

_____

6. ¿Qué mascara de subred utilizará la subred LAN de VLAN 30?

_____

7. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de VLAN 40?

_____

8. ¿Qué mascara de subred utilizará la subred LAN de VLAN 40?

_____

9. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de VLAN 50?

_____

10. ¿Qué mascara de subred utilizará la subred LAN de VLAN 50?

_____

11. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de VLAN 60?

_____

12. ¿Qué mascara de subred utilizará la subred LAN de VLAN 60?

_____

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER Y SWITCH.

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET Y GIGABITETHERNET.

TAREA 4: CONFIGURAR VTP EN LOS SWITCHES.

TAREA 5: CONFIGURAR LAS VLAN EN LOS SERVIDORES VTP Y CONFIGURAR LOS PUERTOS DE LOS ENLACE TRONCALES CON ETHERHANNEL.

TAREA 6: CONFIGURAR LA INTERFAZ DE ENLACES TRONCALES EN R1, R2 Y RA.

TAREA 7: CONFIGURE EL PROTOCOLO EIGRP EN LOS ROUTER R1, R2 Y RA.

TAREA 8: CONFIGURE DHCP EN LOS ROUTERS R1, R2 Y RA.

TAREA 9: CONFIGURAR LOS EQUIPOS DE HOST.

TAREA 10: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

TAREA 11: ANALIS DEL TRAFICO DE PAQUETES

DESAFIO 5.9: VOIP

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet y GigabitEhernet.
- Configurar VOIP.
- Configurar DHCP.
- Configurar el enrutamiento OSPF.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

DIAGRAMA DE TOPOLOGIA

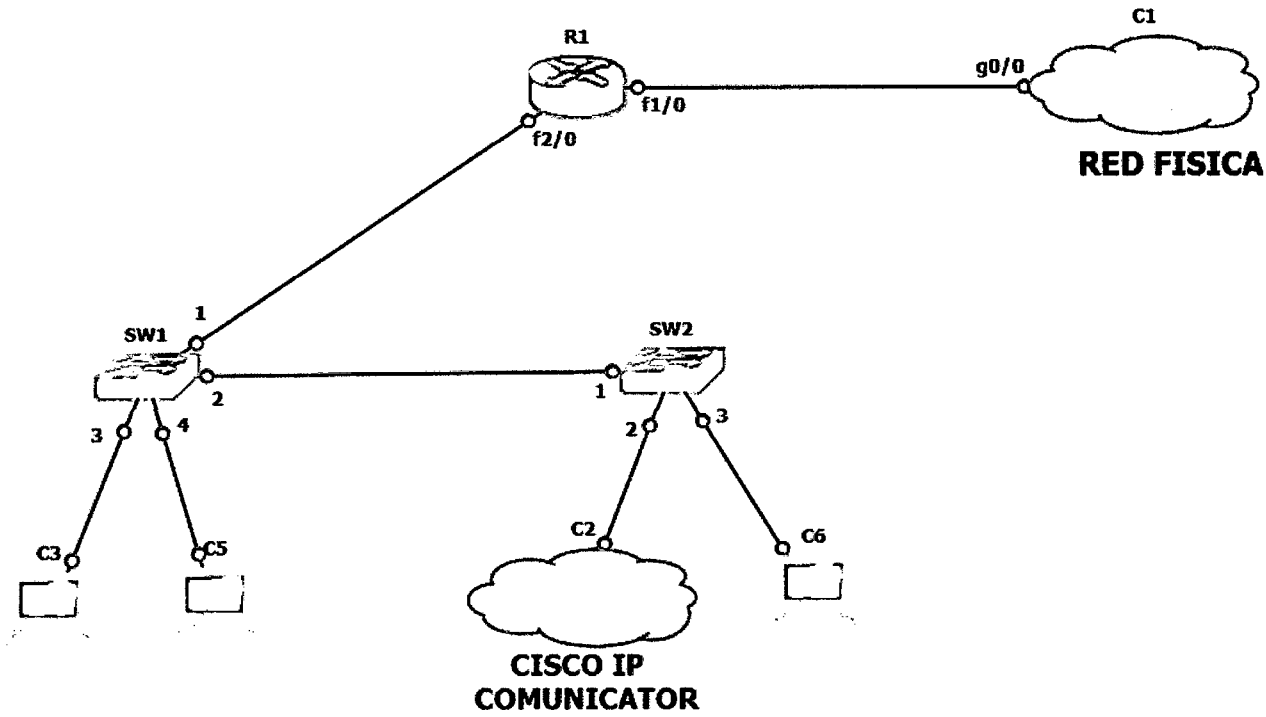


Fig. 5.9.1 Red Virtual en GNS3

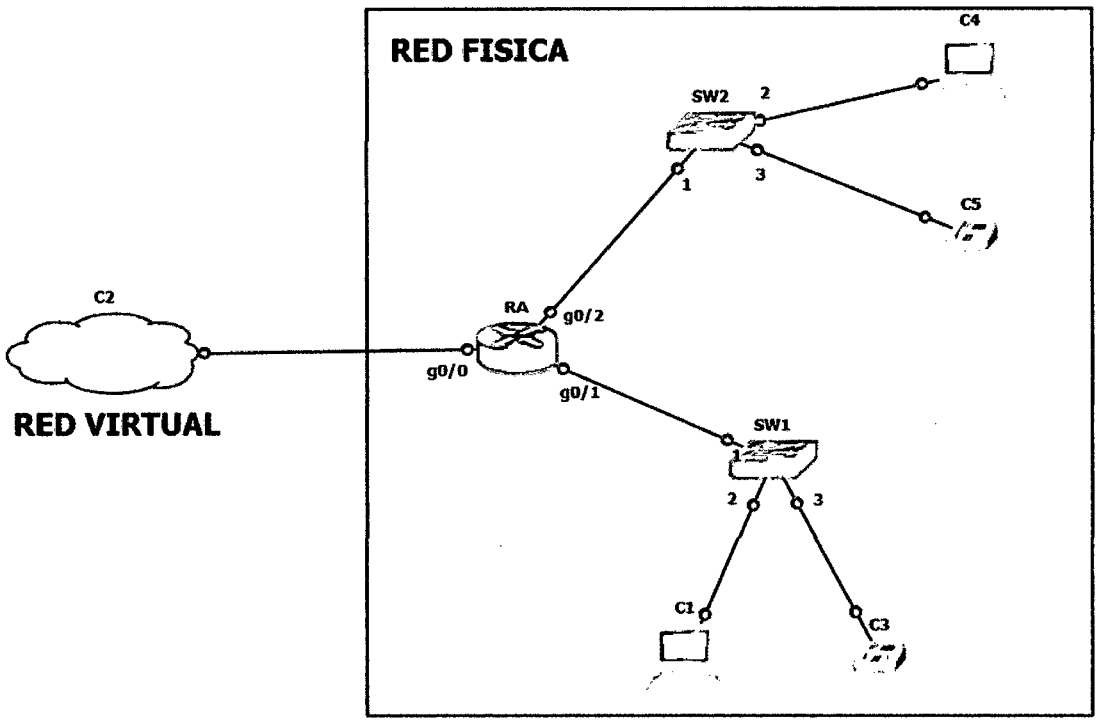


Fig. 5.9.2 Red Física

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	f1/0			No aplicable
	f2/0			No aplicable
ROUTER FISICO	g0/0			No aplicable
	g0/1			No aplicable
	g0/2			No aplicable
C1	NIC	DHCP	DHCP	DHCP
C2	BUCLE INVERTIDO	DHCP	DHCP	DHCP
C3	VPCS	DHCP	DHCP	DHCP
C4	NIC	DHCP	DHCP	DHCP
C5	VPCS	DHCP	DHCP	DHCP
C6	VPCS	DHCP	DHCP	DHCP

Tabla 5.9.1 Direccionamiento IP para las Redes

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Configurar ID de proceso 50, Utilice la dirección **10.0.0.0/30** entre el router **R1-RA**, además teniendo los siguientes requisitos:

LAN R1 – interface f2/0: 160.10.0.0/16 (DHCP)
LAN RA – interface g0/1: 170.10.0.0/16 (DHCP)
LAN RA – interface g0/2: 180.10.0.0/16 (DHCP)

Números telefónicos:

C2:300

C3:400

C5:401

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

TAREA 3: TAREA 3: CONFIGURAR INTERFACES, DHCP Y SERVICIO DE TELEFONIA.

TAREA 4: CONFIGURAR ENRUTAMIENTO OSPF.

TAREA 5: CONFIGURAR DIAL-PEER.

TAREA 6: CONFIGURAR LOS EQUIPOS DE HOST.

TAREA 7: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

TAREA 8: ANALIS DEL TRAFICO DE PAQUETES.

DESAFIO 5.10: CONFIGURACIÓN BÁSICA DE PPP

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red según el diagrama de topología.
- Realizar tareas de configuración básica en los routers.
- Configurar y activar interfaces.
- Configurar el enrutamiento OSPF en todos los routers.
- Configurar la encapsulación PPP en todas las interfaces seriales.
- Configurar la autenticación CHAP y PAP de PPP.
- Aprender acerca de los comandos **debug ppp negotiation y debug ppp authentication**.
- Probar conectividad en la red y funcionamiento de PPP.
- Aprender cómo cambiar la encapsulación en las interfaces seriales de PPP a HDLC.
- Análisis de tráfico de paquetes.

DIAGRAMA DE TOPOLOGIA

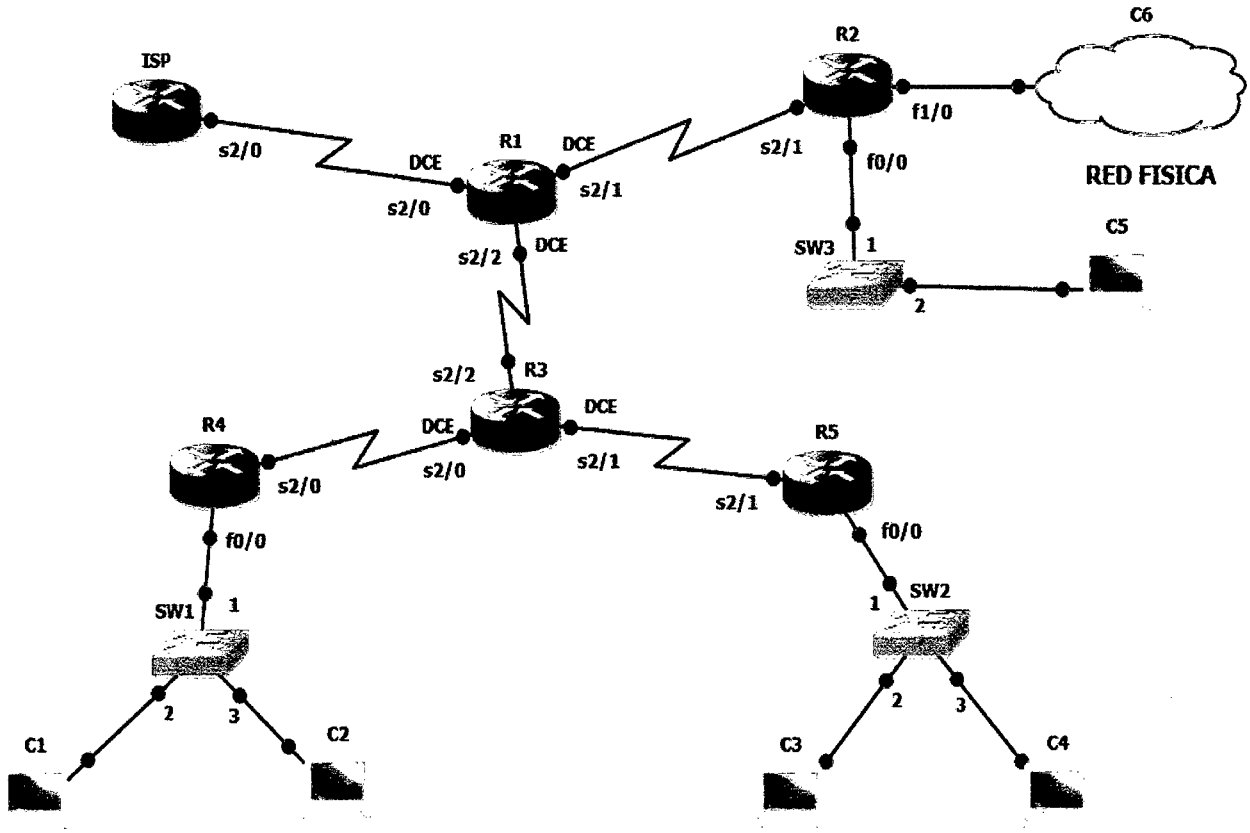


Fig. 5.10.1 Red virtual en GNS3.

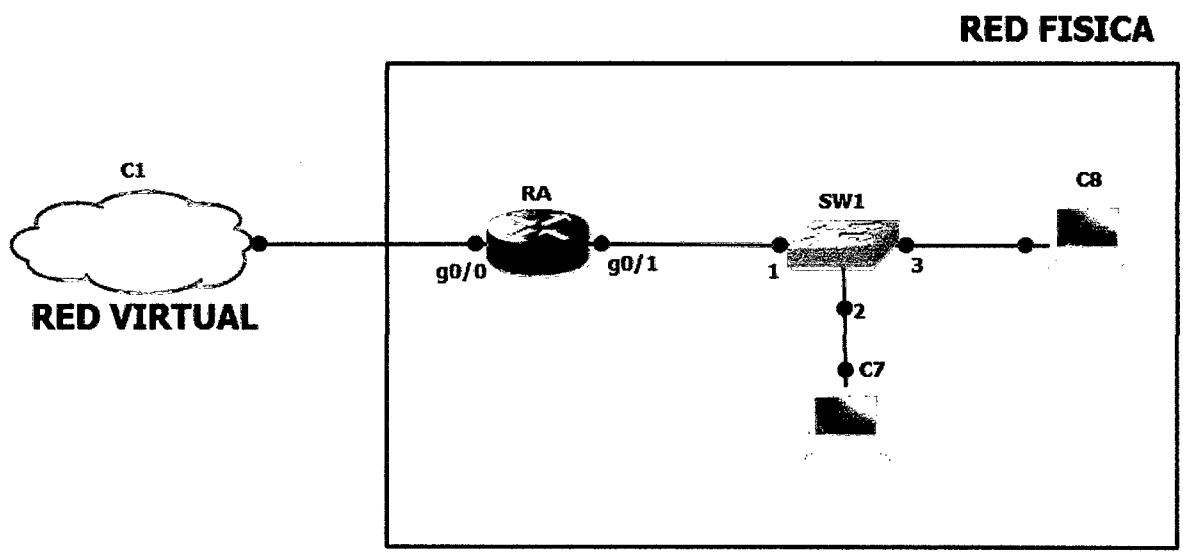


Fig. 5.10.2 Red Física.

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s2/0			
	s2/1			
	s2/2			
R2	s2/1			
	f0/0			
	f1/0			
R3	s2/0			
	s2/1			
	s2/2			
R4	s2/0			
	f0/0			
R5	f0/0			
	s2/1			
ISP	s0/0			
RA	g0/0			
	g0/1			
C1	BUCLE INVERTIDO			
C2	VPCS			
C3	VPCS			
C4	VPCS			
C5	VPCS			
C7	NIC			
C8	NIC			

Tabla 5.10.1 Tabla de direccionamiento IP para las redes.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **100.100.0.0/16** para obtener el direccionamiento IP para las conexiones entre routers, y también para proporcionar direcciones para las 4 LAN:

- LAN R2: 50 host.
- LAN R4: 100
- LAN R5: 120 host.
- LAN Router físico: 200 host.

Para la dirección WAN del ISP y R1 utilice la dirección 200.200.200.0/30.

PASO 1: Asignar las direcciones de subred, según los siguientes requisitos:

82. Asigne la subred 0 de la red 100.100.0.0/16 al enlace entre R1 y ISP.
83. Asigne la subred 1 de la red 100.100.0.0/16 al enlace entre R1 y R2.
84. Asigne la subred 2 de la red 100.100.0.0/16 al enlace entre R1 y R3.
85. Asigne la subred 3 de la red 100.100.0.0/16 al enlace entre R3 y R4.
86. Asigne la subred 4 de la red 100.100.0.0/16 al enlace entre R3 y R5.
87. Asigne la subred 5 de la red 100.100.0.0/16 al enlace entre R2 y RA.
88. Asigne la subred 0 de la red 100.100.0.0/16 a la LAN R4.
89. Asigne la subred 1 de la red 100.100.0.0/16 a la LAN R5.
90. Asigne la subred 2 de la red 100.100.0.0/16 a la LAN R2.
91. Asigne la subred 3 de la red 100.100.0.0/16 a la LAN RA.

Red: 100.100.0.0/16	
Enlace entre:	N° Subred
R1-ISP	Subred 0 :
R1-R2	Subred 1 :
R1-R3	Subred 2 :
R3-R4	Subred 3 :
R3-R5	Subred 4 :
R2-RA	Subred 5 :

Tabla 5.10.2 Asignación de subredes.

Red: 100.100.0.0/16	
LAN	N° Subred
R2	Subred 0 :
R4	Subred 1 :
R5	Subred 2 :
RA	Subred 3 :

Tabla 5.10.3 Asignación de subredes.

PASO 2: Responder las siguientes preguntas.

1. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R2?

_____

2. ¿Qué mascara de subred utilizará la subred LAN de R2?

_____

3. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R4?

_____

4. ¿Qué mascara de subred utilizará la subred LAN de R4?

_____

5. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R5?

_____

6. ¿Qué mascara de subred utilizará la subred LAN de R5?

_____

7. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de RA?

_____

8. ¿Qué mascara de subred utilizará la subred LAN de RA?

_____

9. ¿Cuántas subredes es necesario crear de la red 100.100.0.0/16?

_____

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET Y GIGABITETHERNET.

TAREA 4: CONFIGURAR EL PROTOCOLO DE ENRUTAMIENTO OSPF EN LOS ROUTERS.

TAREA 5: CONFIGURAR LA ENCAPSULACIÓN Y AUTENTICACIÓN PPP PAP Y PPP CHAP EN LAS INTERFACES SERIALES.

TAREA 6: CONFIGURAR LOS EQUIPOS DE HOST.

TAREA 7: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

TAREA 8: ANALIS DEL TRAFICO DE PAQUETES.

DESAFIO 5.11: CONFIGURACION BASICA DE FRAME RELAY

OBJETIVOS DE APRENDIZAJE

Al completar esta práctica de laboratorio, el usuario podrá:

- Conectar una red según el diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar interfaces.
- Configurar el enrutamiento EIGRP en todos los routers.
- Configurar la encapsulación Frame Relay en todas las interfaces seriales.
- Configurar una subinterfaz Frame Relay.
- Configurar un switch Frame Relay.
- Comprender los resultados de los comandos show frame-relay.
- Aprender los efectos del comando debug frame-relay lmi.
- Probar conectividad en la red y funcionamiento de Frame Relay.
- Análisis de tráfico de paquetes.

DIAGRAMA DE TOPOLOGIA:

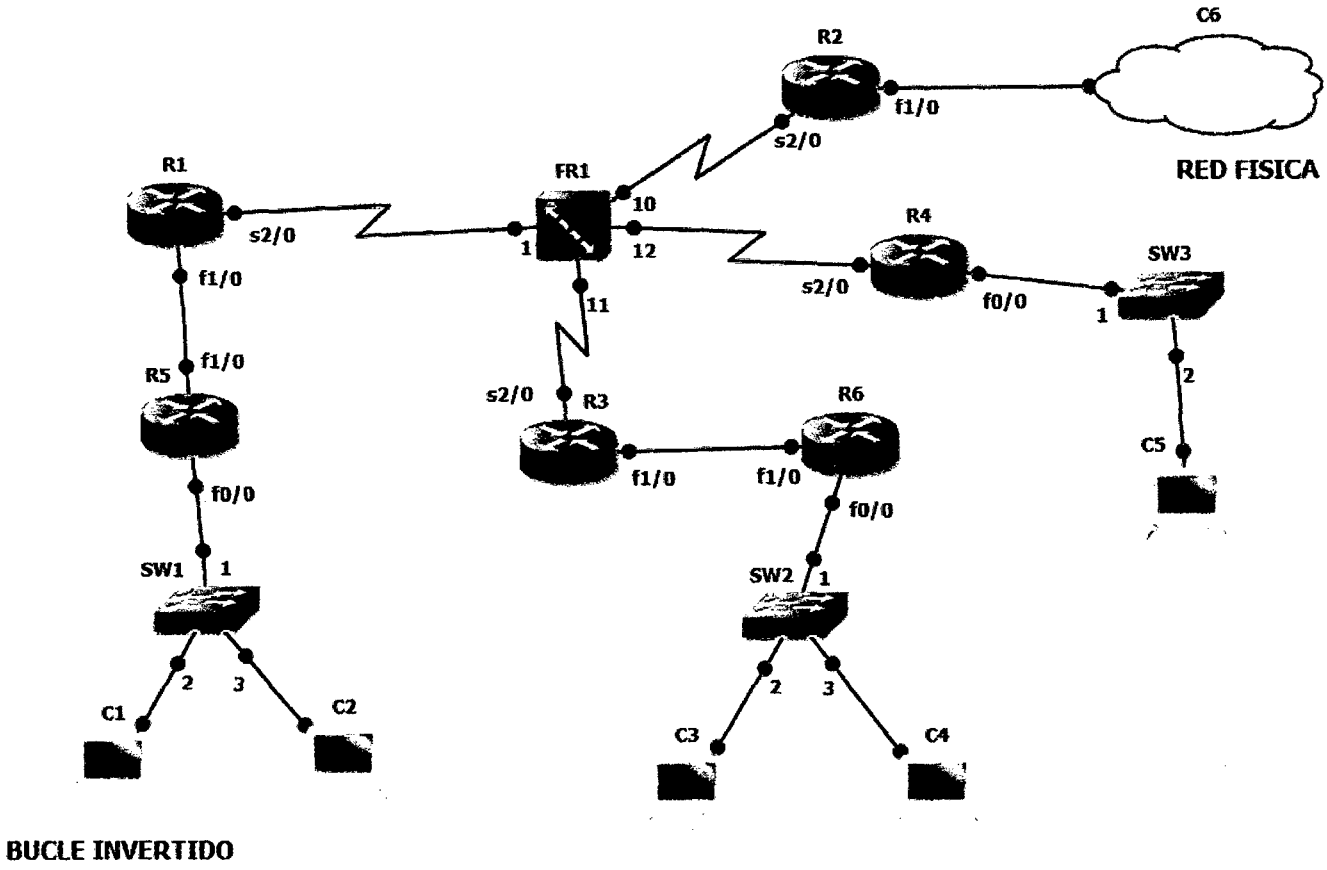


Fig. 5.11.1 Red vistual en GNS3.

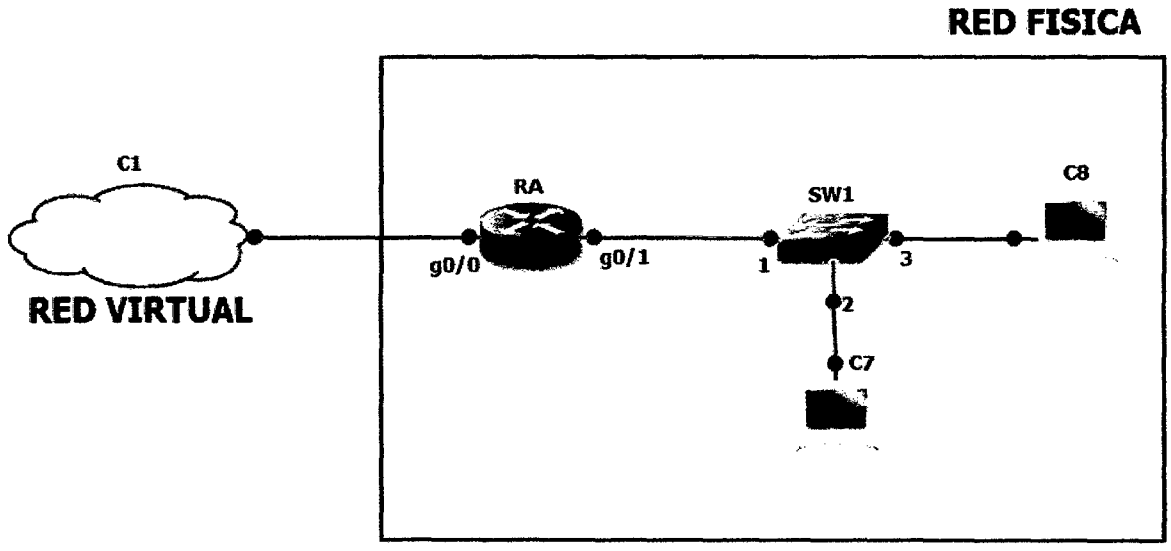


Fig. 5.11.2 Red Física.

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s2/0			
	f1/0			
R2	s2/0			
	f1/0			
R3	s2/0			
	f1/0			
R4	s2/0			
	f0/0			
R5	f0/0			
	f1/0			
R6	f0/0			
	f1/0			
RA	g0/0			
	g0/1			
C1	BUCLE INVERTIDO			
C2	VPCS			
C3	VPCS			
C4	VPCS			
C5	VPCS			
C7	NIC			
C8	NIC			

Tabla 5.11.1 Tabla de direccionamiento IP para las redes.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **110.110.0.0/16** para obtener el direccionamiento IP para las conexiones entre routers, y también para proporcionar direcciones para las 4 LAN:

- LAN R4: 80 host.
- LAN R5: 160
- LAN R6: 120 host.
- LAN Router físico: 220 host.

PASO 1: Asignar las direcciones de subred, según los siguientes requisitos:

92. Asigne la subred 0 de la red 110.110.0.0/16 al enlace entre R1 y R5.
93. Asigne la subred 1 de la red 110.110.0.0/16 al enlace entre R1 y R2.
94. Asigne la subred 2 de la red 110.110.0.0/16 al enlace entre R2 y RA.
95. Asigne la subred 3 de la red 110.110.0.0/16 al enlace entre R1 y R4.
96. Asigne la subred 4 de la red 110.110.0.0/16 al enlace entre R1 y R3.
97. Asigne la subred 5 de la red 110.110.0.0/16 al enlace entre R3 y R6.
98. Asigne la subred 0 de la red 110.110.0.0/16 a la LAN R4.
99. Asigne la subred 1 de la red 110.110.0.0/16 a la LAN R5.
100. Asigne la subred 2 de la red 110.110.0.0/16 a la LAN R6.
101. Asigne la subred 3 de la red 110.110.0.0/16 a la LAN RA.

Red: 110.110.0.0/16	
Enlace entre:	N° Subred
R1-R5	Subred 0 :
R1-R2	Subred 1 :
R2-RA	Subred 2 :
R1-R4	Subred 3 :
R1-R3	Subred 4 :
R3-R6	Subred 5 :

Tabla 5.11.2 Asignación de subredes.

Red: 110.110.0.0/16	
LAN	N° Subred
R4	Subred 0 :
R5	Subred 1 :
R6	Subred 2 :
RA	Subred 3 :

Tabla 5.11.3 Asignación de subredes.

PASO 2: Responder las siguientes preguntas.

1. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R4?

_____

2. ¿Qué mascara de subred utilizará la subred LAN de R4?

_____

3. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R5?

_____

4. ¿Qué mascara de subred utilizará la subred LAN de R5?

_____

5. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R6?

_____

6. ¿Qué mascara de subred utilizará la subred LAN de R5?

_____

7. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de RA?

_____

8. ¿Qué mascara de subred utilizará la subred LAN de RA?

_____

9. ¿Cuántas subredes es necesario crear de la red 110.110.0.0/16?

_____

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET Y GIGABITETHERNET.

TAREA 4: CONFIGURAR SWITCH Y ROUTERS CON FRAME RELAY.

TAREA 5: CONFIGURAR EL PROTOCOLO DE ENRUTAMIENTO OSPF EN LOS ROUTERS.

TAREA 6: CONFIGURAR LOS EQUIPOS DE HOST.

TAREA 7: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

TAREA 8: ANALIS DEL TRAFICO DE PAQUETES.

DESAFIO 5.12: MPLS LDP

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet y GigabitEhernet.
- Configurar MPLS y el protocolo de distribución de etiquetas LDP.
- Configurar el enrutamiento BGP.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

DIAGRAMA DE TOPOLOGIA

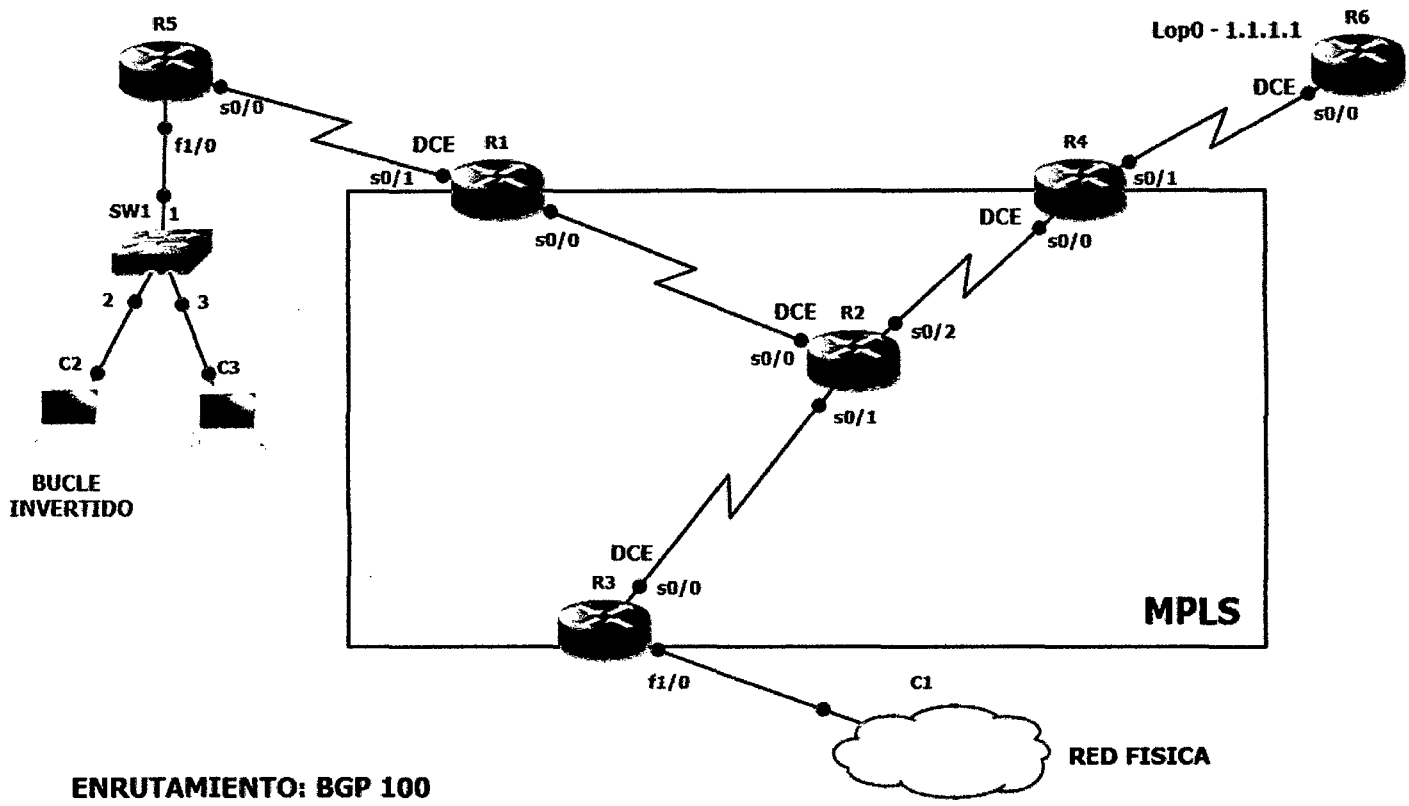


Fig. 5.12.1 Red Virtual en GNS3

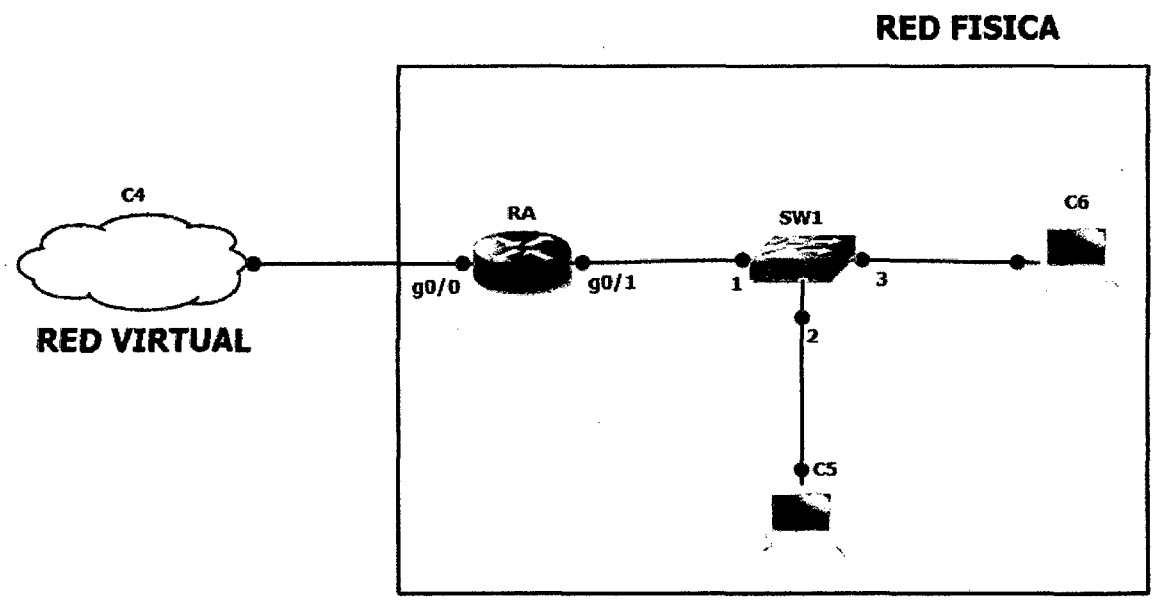


Fig. 5.12.2 Red Física

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s0/0			
	s0/1			
R2	s0/0			
	s0/1			
	s0/2			
R3	s0/0			
	f1/0			
R4	s0/0			
	s0/1			
R5	s0/0			
	f1/0			
R6	s0/0			
RA	g0/0			
	g0/1			
C2	BUCLE INVERTIDO			
C3	VPCS			
C5	NIC			
C6	NIC			

Tabla 5.12.1 Direccionamiento IP para las Redes

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Configurar sistema autónomo 200, La red **30.0.0.0/8** debe dividirse en subredes para obtener direccionamiento IP usando VLSM para los enlaces entre routers, además dividir la red **170.20.0.0/16** para proporcionar direcciones para las 2 LAN:

- LAN de R5 necesitara 150 direcciones.
- LAN de RA necesitara 100 direcciones.

PASO 1: Asignar las direcciones de subred, según los siguientes requisitos:

102. Asigne la subred 0 de la red 30.0.0.0/8 al enlace entre R1 y R2.
103. Asigne la subred 1 de la red 30.0.0.0/8 al enlace entre R1 y R5.
104. Asigne la subred 2 de la red 30.0.0.0/8 al enlace entre R2 y R3.
105. Asigne la subred 3 de la red 30.0.0.0/8 al enlace entre R2 y R4.
106. Asigne la subred 4 de la red 30.0.0.0/8 al enlace entre R3 y RA.
107. Asigne la subred 5 de la red 30.0.0.0/8 al enlace entre R4 y R6.
108. Asigne la subred 0 de la red 170.20.0.0/16 a la LAN RA.
109. Asigne la subred 1 de la red 170.20.0.0/16 a la LAN R5.

Red: 30.0.0.0/8	
Enlace entre:	N° Subred
R1-R2	Subred 0 :
R1-R5	Subred 1 :
R2-R3	Subred 2 :
R2-R4	Subred 3 :
R3-RA	Subred 4 :
R4-R6	Subred 5 :

Tabla 5.12.2 Asignación de subredes

Red: 170.20.0.0/16	
LAN	N° Subred
RA	Subred 0 :
R5	Subred 1 :

Tabla 5.12.3 Asignación de subredes

PASO 2: Responder las siguientes preguntas.

1. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de RA?

---

2. ¿Qué mascara de subred utilizará la subred LAN de RA?

---

3. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R5?

---

4. ¿Qué mascara de subred utilizará la subred LAN de R5?

---

5. ¿Cuántas subredes es necesario crear de la red 170.20.0.0/16?

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET.

TAREA 4: CONFIGURAR BGP.

TAREA 5: CONFIGURAR MPLS.

TAREA 6: CONFIGURAR LOS EQUIPOS DE HOST.

TAREA 7: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

TAREA 8: ANALIS DEL TRAFICO DE PAQUETES

DESAFIO 5.13: CONFIGURACION BASICA DE DHCP Y NAT

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, el usuario podrá:

- Preparar la red.
- Realizar las configuraciones básicas del router.
- Configurar un servidor de DHCP del IOS de Cisco.
- Configurar el enrutamiento estático y por defecto.
- Configurar NAT estática.
- Configurar NAT dinámica con un conjunto de direcciones.
- Configurar la sobrecarga de NAT.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

DIAGRAMA DE TOPOLOGIA

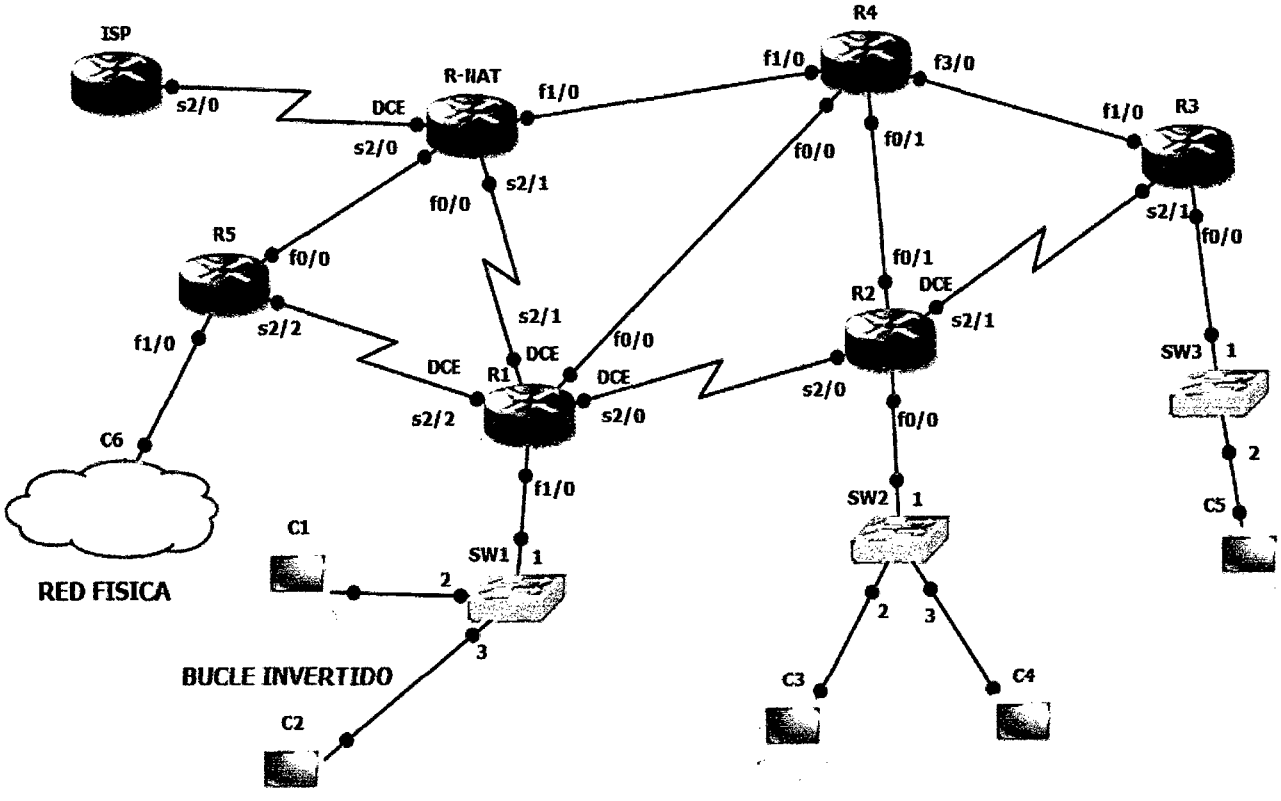


Fig. 5.13.1 Red virtual en GNS3.

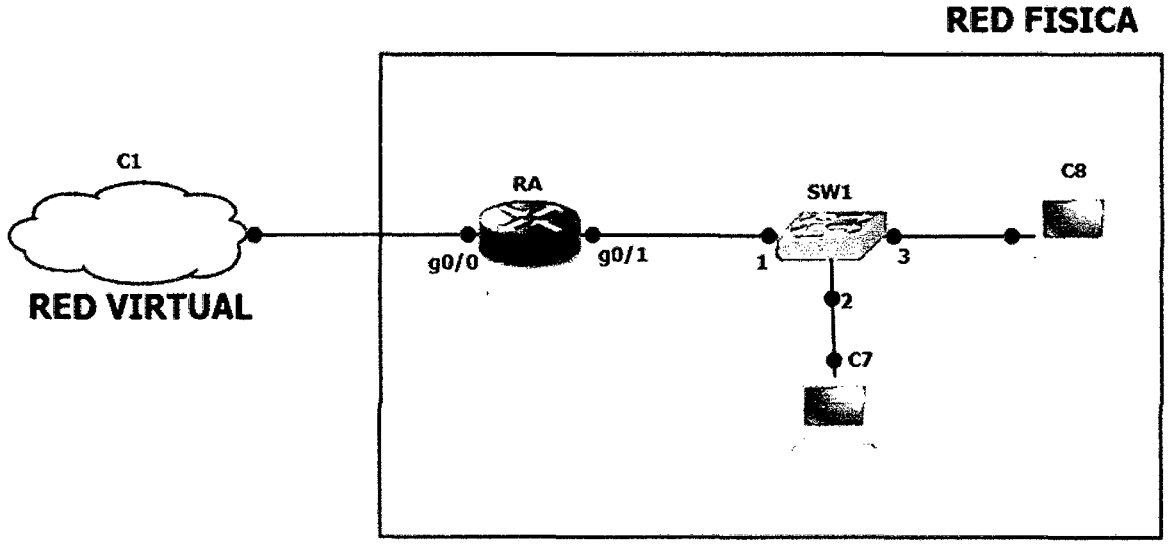


Fig. 5.13.2 Red Física.

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s2/0			
	s2/1			
	s2/2			
	f0/0			
	f1/0			
R2	s2/0			
	s2/1			
	f0/1			
R3	s2/1			
	f0/0			
	f1/0			
R4	f0/0			
	f0/1			
	f1/0			
	f3/0			
R5	f0/0			
	f1/0			
	s2/2			
R-NAT	s0/0			
	s2/1			
	f0/0			
	f1/0			
ISP	s0/0			
RA	g0/0			
	g0/1			
C1	BUCLE INVERTIDO			
C2	VPCS			
C3	VPCS			
C4	VPCS			
C5	VPCS			
C7	NIC			
C8	NIC			

Tabla 5.13.1 Tabla de direccionamiento IP para las redes.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **172.16.0.0/16** para obtener el direccionamiento IP para las conexiones entre routers, y también para proporcionar direcciones para las 4 LAN:

- LAN R1: 180 host.
- LAN R2: 100 host.
- LAN R3: 80 host.
- LAN Router físico: 220 host.

Para la dirección WAN del ISP y R-NAT utilice la dirección 200.200.200.0/30.

PASO 1: Asignar las direcciones de subred, según los siguientes requisitos:

110. Asigne la subred 0 de la red 172.16.0.0/16 al enlace entre ISP y R-NAT.
111. Asigne la subred 1 de la red 172.16.0.0/16 al enlace entre R-NAT y R5.
112. Asigne la subred 2 de la red 172.16.0.0/16 al enlace entre R-NAT y R1.
113. Asigne la subred 3 de la red 172.16.0.0/16 al enlace entre R-NAT y R4.
114. Asigne la subred 4 de la red 172.16.0.0/16 al enlace entre R5 y RA.
115. Asigne la subred 5 de la red 172.16.0.0/16 al enlace entre R5 y R1.
116. Asigne la subred 6 de la red 172.16.0.0/16 al enlace entre R1 y R2.
117. Asigne la subred 7 de la red 172.16.0.0/16 al enlace entre R4 y R1.
118. Asigne la subred 8 de la red 172.16.0.0/16 al enlace entre R4 y R2.
119. Asigne la subred 9 de la red 172.16.0.0/16 al enlace entre R4 y R3.
120. Asigne la subred 10 de la red 172.16.0.0/16 al enlace entre R2 y R3.
121. Asigne la subred 0 de la red 172.16.0.0/16 a la LAN R1.
122. Asigne la subred 1 de la red 172.16.0.0/16 a la LAN R2.
123. Asigne la subred 2 de la red 172.16.0.0/16 a la LAN R3.
124. Asigne la subred 4 de la red 172.16.0.0/16 a la LAN RA.

Red: 172.16.0.0/16	
Enlace entre:	N° Subred
ISP-R-NAT	Subred 0 :
R-NAT-R5	Subred 1 :
R-NAT-R1	Subred 2 :
R-NAT-R4	Subred 3 :
R5-RA	Subred 4 :
R5-R1	Subred 5 :
R1-R2	Subred 6 :
R4-R1	Subred 7 :
R4-R2	Subred 8 :
R4-R3	Subred 9 :
R2-R3	Subred 10 :

Tabla 5.13.2 Asignación de subredes.

Red: 172.16.0.0/16	
LAN	N° Subred
R1	Subred 0 :
R2	Subred 1 :
R3	Subred 2 :
RA	Subred 3 :

Tabla 5.13.3 Asignación de subredes.

PASO 2: Responder las siguientes preguntas.

1. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R1?

---

2. ¿Qué mascara de subred utilizará la subred LAN de R1?

---

3. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R2?

---

4. ¿Qué mascara de subred utilizará la subred LAN de R2?

5. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R4?

6. ¿Qué mascara de subred utilizará la subred LAN de R3?

7. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de RA?

8. ¿Qué mascara de subred utilizará la subred LAN de RA?

9. ¿Cuántas subredes es necesario crear de la red 172.16.0.0/16?

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET Y GIGABITETHERNET.

TAREA 4: CONFIGURAR EL PROTOCOLO DE ENRUTAMIENTO OSPF.

TAREA 5: CONFIGURE DHCP EN EL ROUTER R-DHCP.

TAREA 6: CONFIGURAR NAT ÉSTATICA, DINÁMICA Y PAT.

TAREA 7: CONFIGURAR LOS EQUIPOS DE HOST.

TAREA 8: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

TAREA 9: ANALIS DEL TRAFICO DE PAQUETES.

DESAFIO 5.14: CONFIGURACIÓN BÁSICA DE LISTAS DE CONTROL DE ACCESO (ACL)

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, el usuario podrá:

- Conectar una red según el diagrama de topología.
- Realizar tareas de configuración básica en los routers.
- Configurar y activar interfaces.
- Configurar el enrutamiento OSPF en todos los routers.
- Diseñar ACL nombradas estándar y nombradas ampliadas.
- Aplicar ACL nombradas estándar y nombradas ampliadas.
- Probar ACL nombradas estándar y nombradas ampliadas.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

DIAGRAMA DE TOPOLOGIA

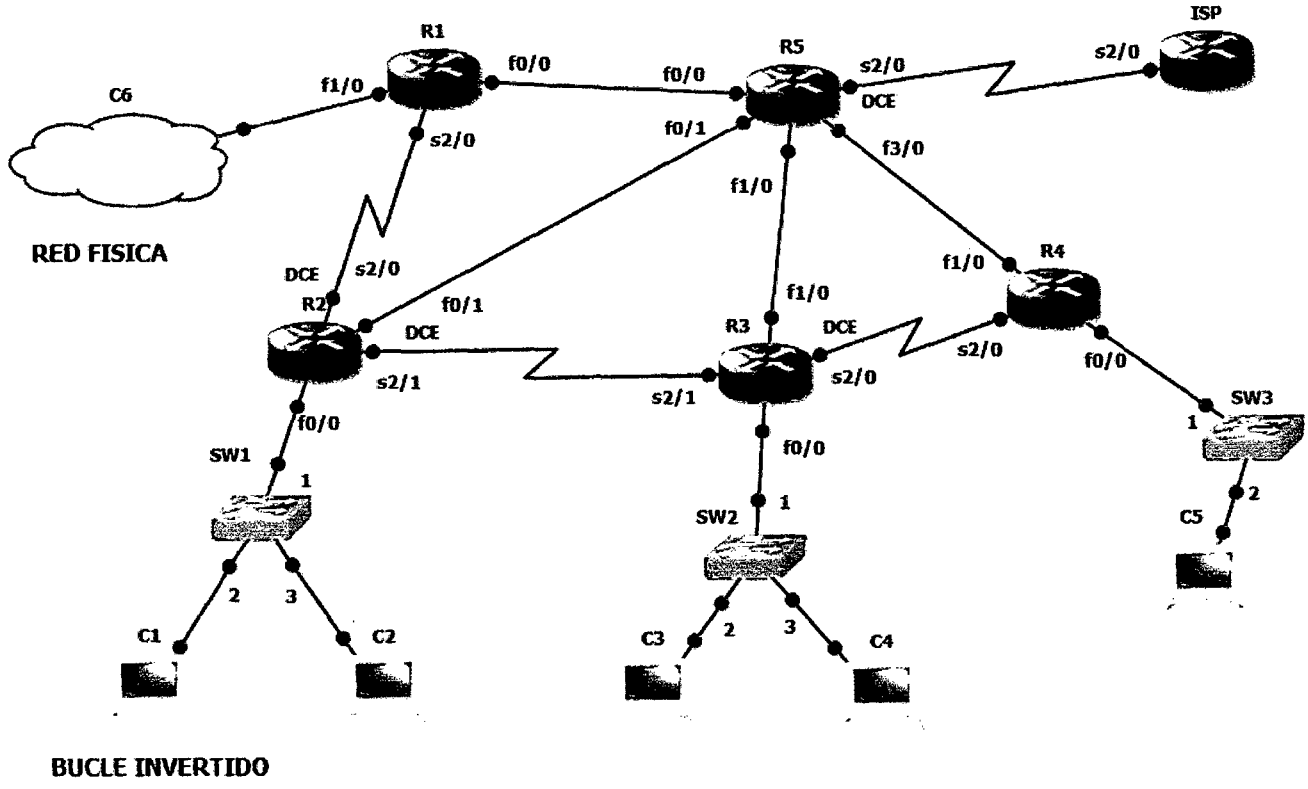


Fig. 5.14.1 Red virtual en GNS3.

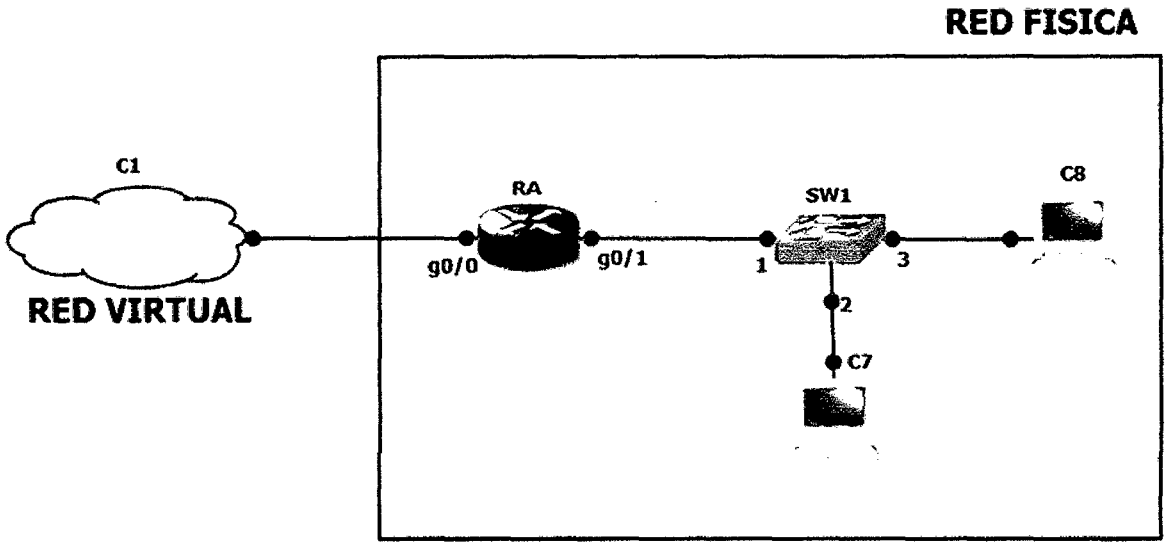


Fig. 5.14.2 Red Física.

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s2/0			
	f0/0			
	f1/0			
R2	s2/0			
	s2/1			
	f0/1			
R3	s2/0			
	s2/1			
	f1/0			
R4	f0/0			
	f1/0			
	s2/0			
R5	s2/0			
	f0/0			
	f0/1			
	f1/0			
	f3/0			
ISP	s2/0			
RA	g0/0			
	g0/1			
C1	BUCLE INVERTIDO			
C2	VPCS			
C3	VPCS			
C4	VPCS			
C5	VPCS			
C6	VPCS			
C8	NIC			
C9	NIC			

Tabla 5.14.1 Tabla de direccionamiento IP para las redes.

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Utilice la dirección **172.16.0.0/16** para obtener el direccionamiento IP para las conexiones entre routers, y también para proporcionar direcciones para las 4 LAN:

- LAN R2: 200 host.
- LAN R3: 100 host.
- LAN R4: 80 host.
- LAN Router físico: 220 host.

Para la dirección WAN del ISP y R5 utilice la dirección 200.200.200.0/30.

PASO 1: Asignar las direcciones de subred, según los siguientes requisitos:

125. Asigne la subred 0 de la red 172.16.0.0/16 al enlace entre R1 y RA.
126. Asigne la subred 1 de la red 172.16.0.0/16 al enlace entre R1 y R2.
127. Asigne la subred 2 de la red 172.16.0.0/16 al enlace entre R1 y R5.
128. Asigne la subred 3 de la red 172.16.0.0/16 al enlace entre R5 y R2.
129. Asigne la subred 4 de la red 172.16.0.0/16 al enlace entre R5 y R3.
130. Asigne la subred 5 de la red 172.16.0.0/16 al enlace entre R5 y R4.
131. Asigne la subred 6 de la red 172.16.0.0/16 al enlace entre R2 y R3.
132. Asigne la subred 7 de la red 172.16.0.0/16 al enlace entre R3 y R4.
133. Asigne la subred 8 de la red 172.16.0.0/16 al enlace entre R5 y ISP.
134. Asigne la subred 0 de la red 172.16.0.0/16 a la LAN R2.
135. Asigne la subred 1 de la red 172.16.0.0/16 a la LAN R3.
136. Asigne la subred 2 de la red 172.16.0.0/16 a la LAN R4.
137. Asigne la subred 3 de la red 172.16.0.0/16 a la LAN RA.

Red: 172.16.0.0/16	
Enlace entre:	N° Subred
R1-RA	Subred 0 :
R1-R2	Subred 1 :
R1-R5	Subred 2 :
R5-R2	Subred 3 :
R5-R3	Subred 4 :
R5-R4	Subred 5 :
R2-R3	Subred 6 :
R3-R4	Subred 7:
R5-ISP	Subred 8 :

Tabla 5.14.2 Asignación de subredes.

Red: 172.16.0.0/16	
LAN	N° Subred
R2	Subred 0 :
R3	Subred 1 :
R4	Subred 2 :
RA	Subred 3:

Tabla 5.14.3 Asignación de subredes.

PASO 2: Responder las siguientes preguntas.

1. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R2?

_____

2. ¿Qué mascara de subred utilizará la subred LAN de R2?

_____

3. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R3?

_____

4. ¿Qué mascara de subred utilizará la subred LAN de R3?

_____

5. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R4?

_____

6. ¿Qué mascara de subred utilizará la subred LAN de R4?

_____

7. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de RA?

_____

8. ¿Qué mascara de subred utilizará la subred LAN de RA?

_____

9. ¿Cuántas subredes es necesario crear de la red 172.16.0.0/16?

_____

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET Y GIGABITETHERNET.

TAREA 4: CONFIGURAR EL PROTOCOLO DE ENRRUTAMIENTO EIGRP.

TAREA 5: CONFIGURAR LAS ACL EN LOS ROUTERS R2 y RA PARA QUE NO TENGAN ACCESO A ELLAS LOS HOST DE LAN DE R3 Y R4.

TAREA 6: CONFIGURAR LOS EQUIPOS DE HOST.

TAREA 7: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

TAREA 8: ANALIS DEL TRAFICO DE PAQUETES.

DESAFIO 5.16: REDISTRIBUCION DE PROTOCOLOS

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet y GigabitEhernet.
- Configurar los protocolos: OSPF, EIGRP y RIPV2.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

DIAGRAMA DE TOPOLOGIA

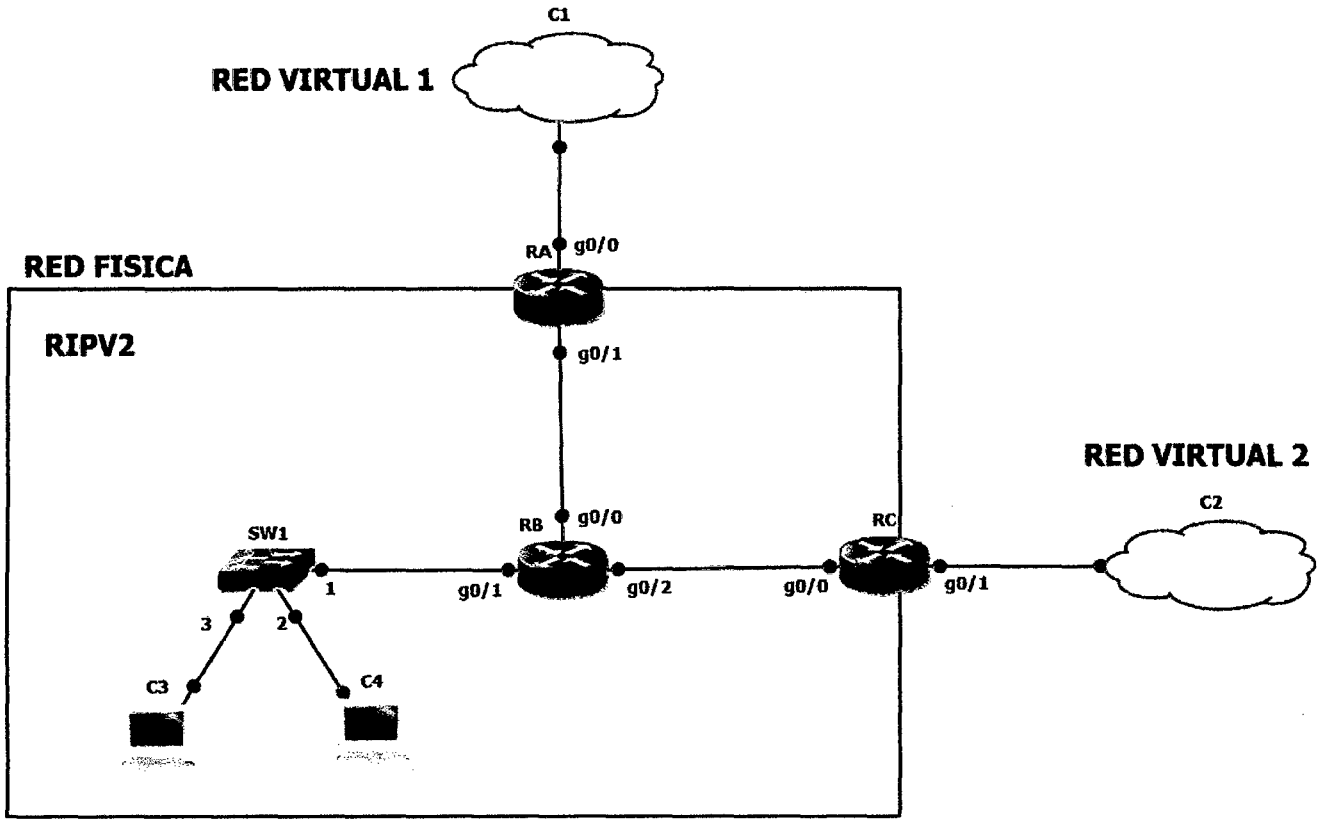


Fig. 5.16.1 Red Física

RED VIRTUAL 1

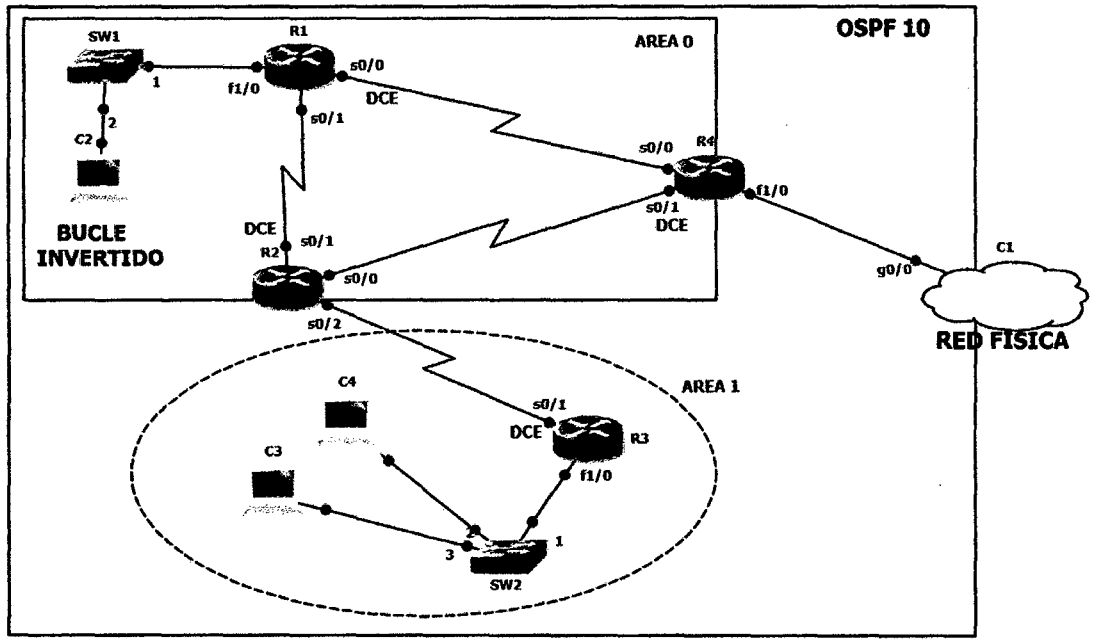


Fig. 5.16.2 Red Virtual 1 en GNS3

RED VIRTUAL 2

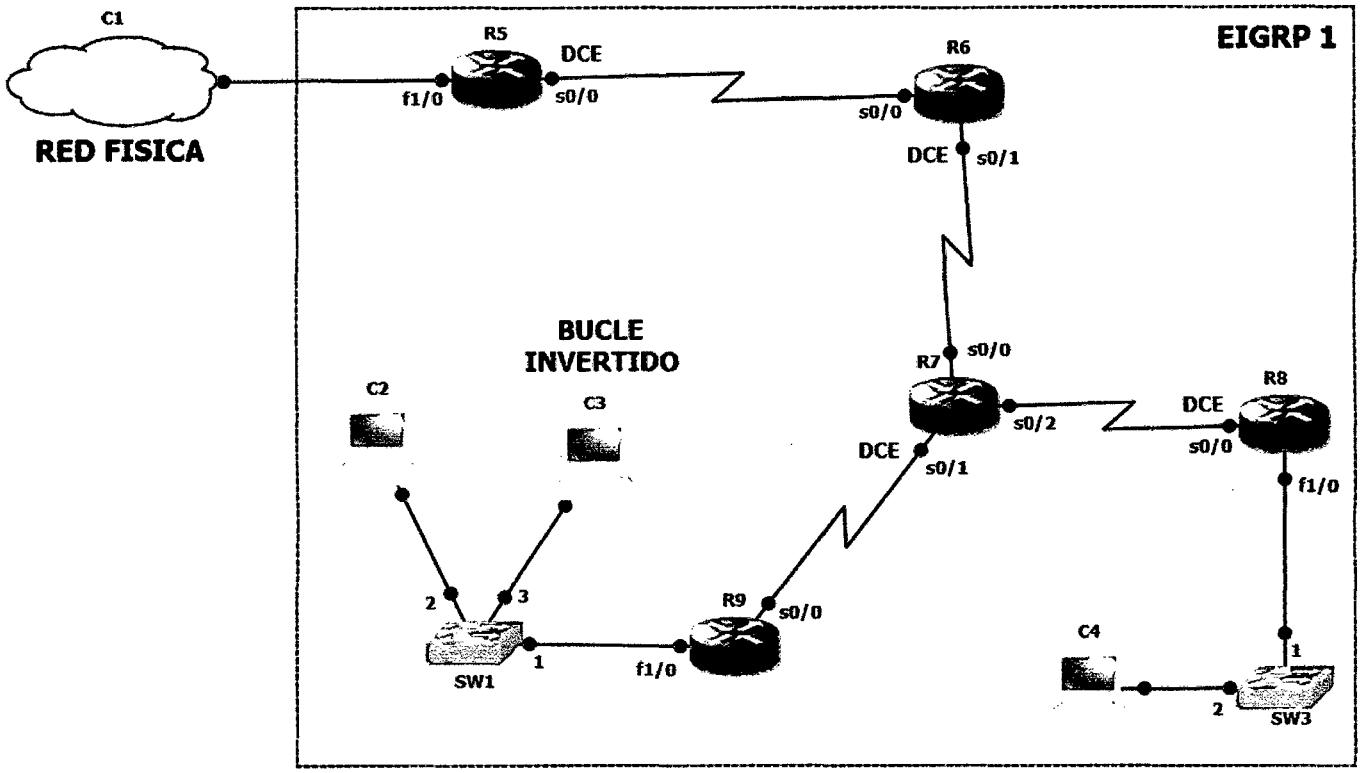


Fig. 5.16.3 Red Virtual 2 en GNS3

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

RED FISICA

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
RA	g0/0			
	g0/1			
RB	g0/0			
	g0/1			
	g0/2			
RC	g0/0			
	g0/1			
C3	NIC			
C4	NIC			

Tabla 5.16.1 Direccionamiento IP para las Redes

RED VIRTUAL 1

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s0/0			
	s0/1			
	f1/0			
R2	s0/0			
	s0/1			
	s0/2			
R3	s0/1			
	f1/0			
R4	s0/0			
	s0/1			
	f1/0			
C2	BUCLE INVERTIDO			
C3	VPCS			
C4	VPCS			

Tabla 5.16.2 Direccionamiento IP para las Redes

RED VIRTUAL 2

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R5	s0/0			
	f1/0			
R6	s0/0			
	s0/1			
R7	s0/0			
	s0/1			
	s0/2			
R8	s0/0			
	f1/0			
R9	s0/0			
	f1/0			
C2	VPCS			
C3	BUCLE INVERTIDO			
C4	VPCS			

Tabla 5.16.3 Direccionamiento IP para las Redes

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. La red **50.0.0.0/8** debe dividirse en subredes para obtener direccionamiento IP usando VLSM para los enlaces entre routers, además dividir la red **140.0.0.0/16** para proporcionar direcciones para las 2 LAN:

- LAN de RB necesitara 200 direcciones.
- LAN de R1 necesitara 1500 direcciones.
- LAN de R3 necesitara 300 direcciones.
- LAN de R8 necesitara 1000 direcciones.
- LAN de R9 necesitara 800 direcciones.

PASO 1: Asignar las direcciones de subred, según los siguientes requisitos:

138. Asigne la subred 0 de la red 50.0.0.0/8 al enlace entre RA y RB.
139. Asigne la subred 1 de la red 50.0.0.0/8 al enlace entre RB y RC.
140. Asigne la subred 2 de la red 50.0.0.0/8 al enlace entre R1 y R2.
141. Asigne la subred 3 de la red 50.0.0.0/8 al enlace entre R1 y R4.
142. Asigne la subred 4 de la red 50.0.0.0/8 al enlace entre R2 y R3.
143. Asigne la subred 5 de la red 50.0.0.0/8 al enlace entre R5 y R6.
144. Asigne la subred 6 de la red 50.0.0.0/8 al enlace entre R6 y R7.
145. Asigne la subred 7 de la red 50.0.0.0/8 al enlace entre R7 y R8.
146. Asigne la subred 8 de la red 50.0.0.0/8 al enlace entre R7 y R9.
147. Asigne la subred 0 de la red 140.0.0.0/16 a la LAN RB.
148. Asigne la subred 1 de la red 140.0.0.0/16 a la LAN R1.
149. Asigne la subred 2 de la red 140.0.0.0/16 a la LAN R3.
150. Asigne la subred 3 de la red 140.0.0.0/16 a la LAN R8.
151. Asigne la subred 4 de la red 140.0.0.0/16 a la LAN R9.

Red: 50.0.0.0/8	
Enlace entre:	N° Subred
RA-RB	Subred 0 :
RB-RC	Subred 1 :
R1-R2	Subred 2 :
R1-R4	Subred 3 :
R2-R3	Subred 4 :
R5-R6	Subred 5 :
R6-R7	Subred 6 :
R7-R8	Subred 7 :
R7-R9	Subred 8 :

Tabla 5.16.4 Asignación de subredes

Red: 140.0.0.0/16	
LAN	N° Subred
RB	Subred 0 :
R1	Subred 1 :
R3	Subred 2 :
R8	Subred 3 :
R9	Subred 4 :

Tabla 5.16.5 Asignación de subredes

PASO 2: Responder las siguientes preguntas.

1. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de RB?

_____

2. ¿Qué mascara de subred utilizará la subred LAN de RB?

_____

3. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R1?

_____

4. ¿Qué mascara de subred utilizará la subred LAN de R1?

_____

5. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R3?

_____

6. ¿Qué mascara de subred utilizará la subred LAN de R3?

_____

7. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R8?

_____

8. ¿Qué mascara de subred utilizará la subred LAN de R8?

_____

9. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R9?

---

10. ¿Qué mascara de subred utilizará la subred LAN de R9?

---

11. ¿Cuántas subredes es necesario crear de la red 140.0.0.0/16?

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET Y GIGABITETHERNET.

TAREA 4: CONFIGURAR PROTOCOLOS DE ENRUTAMIENTO.

TAREA 5: CONFIGURAR PROTOCOLOS DE REDISTRIBUCION.

TAREA 6: CONFIGURAR LOS EQUIPOS DE HOST.

TAREA 7: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

TAREA 8: ANALISIS DEL TRAFICO DE PAQUETES.

DESAFIO 5.17: IPV6

OBJETIVOS DE APRENDIZAJE:

Al completar esta práctica de laboratorio, usted podrá:

- Conectar una red de acuerdo con el Diagrama de topología.
- Realizar tareas de configuración básicas en un router.
- Configurar y activar las interfaces serial, FastEthernet y GigabitEhernet.
- Configurar IPV6 Tunneling.
- Configurar IPV6 RIPNG.
- Configurar OSPF.
- Probar la conectividad.
- Análisis de tráfico de paquetes.

DIAGRAMA DE TOPOLOGIA

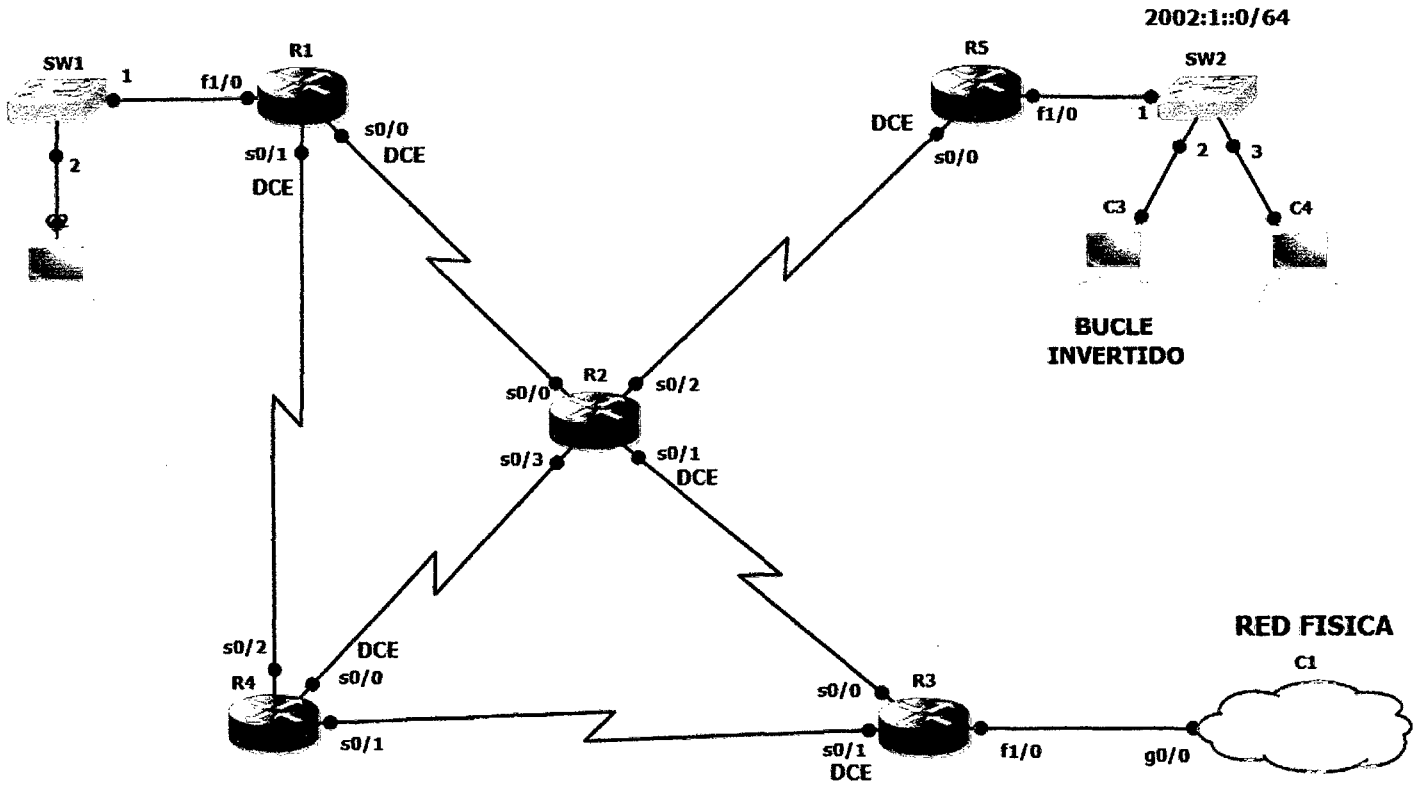


Fig. 5.17.1 Red Virtual en GNS3

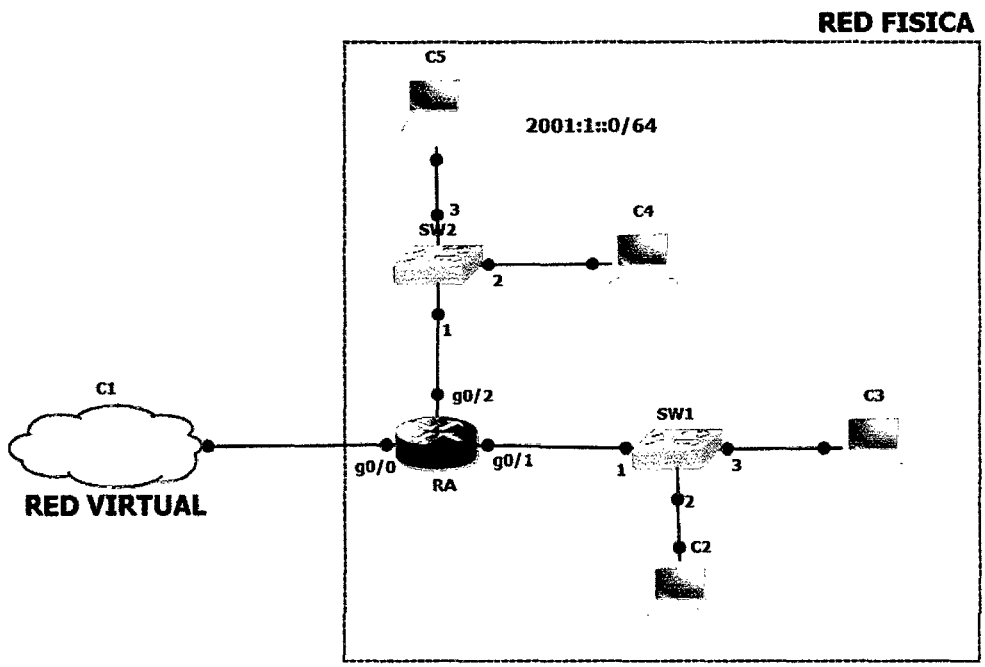


Fig. 5.17.2 Red Física

TABLA DE DIRECCIONAMIENTO IP PARA LAS REDES LAN Y WAN

RED VIRTUAL:

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
R1	s0/0			
	s0/1			
	f1/0			
R2	s0/0			
	s0/1			
	s0/2			
	s0/3			
R3	s0/0			
	s0/1			
	f1/0			
R4	s0/0			
	s0/1			
	s0/2			
R5	s0/0			
	f1/0			
C2	VPCS			
C3	BUCLE INVERTIDO			
C4	VPCS			

Tabla 5.17.1 Direccionamiento IP para las Redes

RED FISICA:

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
RA	g0/0			
	g0/1			
	g0/2			
C2	NIC			
C3	NIC			
C4	NIC			
C5	NIC			

Tabla 5.17.2 Direccionamiento IP para las Redes

ESCENARIO:

En esta actividad de laboratorio, el usuario armará y conectará la red que se muestra en el Diagrama de topología. Configurar ID de proceso 100 en todos los routers, la red **10.0.0.0/8** debe dividirse en subredes para obtener direccionamiento IP usando VLSM para los enlaces entre routers, además dividir la red **192.168.0.0/24** para proporcionar direcciones para las 2 LAN:

- LAN de R1 necesitara 20 direcciones.
- LAN de RA necesitara 35 direcciones.

Utilizar las direcciones 2001:1::0/64 y 2002:1::0/64 para las redes IPV6.

PASO 1: Asignar las direcciones de subred, según los siguientes requisitos:

152. Asigne la subred 0 de la red 10.0.0.0/8 al enlace entre R1 y R2.
153. Asigne la subred 1 de la red 10.0.0.0/8 al enlace entre R1 y R4.
154. Asigne la subred 2 de la red 10.0.0.0/8 al enlace entre R2 y R3.
155. Asigne la subred 3 de la red 10.0.0.0/8 al enlace entre R2 y R4.
156. Asigne la subred 4 de la red 10.0.0.0/8 al enlace entre R3 y R4.
157. Asigne la subred 5 de la red 10.0.0.0/8 al enlace entre R2 y R5.
158. Asigne la subred 6 de la red 10.0.0.0/8 al enlace entre R3 y RA.
159. Asigne la subred 0 de la red 192.168.1.0/24 a la LAN R1.
160. Asigne la subred 1 de la red 192.168.1.0/24 a la LAN RA.

Red: 10.0.0.0/8	
Enlace entre:	N° Subred
R1-R2	Subred 0 :
R1-R4	Subred 1 :
R2-R3	Subred 2 :
R2-R4	Subred 3 :
R3-R4	Subred 4 :
R2-R5	Subred 5 :
R3-RA	Subred 6 :

Tabla 5.17.3 Asignación de subredes

Red: 192.168.1.0/24	
LAN	N° Subred
R1	Subred 0 :
RA	Subred 1 :

Tabla 5.17.4 Asignación de subredes

PASO 2: Responder las siguientes preguntas.

1. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de R1?

_____

2. ¿Qué mascara de subred utilizará la subred LAN de R1?

_____

3. ¿Cuál es la máxima cantidad de dirección host que se pueden asignar en la LAN de RA?

_____

4. ¿Qué mascara de subred utilizará la subred LAN de RA?

_____

5. ¿Cuántas subredes es necesario crear de la red 192.168.1.0/24?

_____

TAREA 1: MONTAR LA RED FISICA Y LA RED EN GNS3.

TAREA 2: REALIZAR LA CONFIGURACION BASICA DEL ROUTER.

TAREA 3: CONFIGURE Y ACTIVE LAS INTERFACES SERIALES, FASTETHERNET Y GIGABITETHERNET CON IPV4.

TAREA 4: CONFIGURAR IPV6.

TAREA 5: CONFIGURAR PROTOCOLO OSPF.

TAREA 6: CONFIGURAR PROTOCOLO RIPNG.

TAREA 7: CONFIGURAR LOS EQUIPOS DE HOST.

TAREA 8: VERIFICAR Y PROBAR LAS CONFIGURACIONES.

TAREA 9: ANALIS DEL TRAFICO DE PAQUETES.

PRESUPUESTOS

DETALLES DEL GASTO	DESCRIPCION	CANTIDAD	MONTO
Bienes	Cable UTP cat 5e	40 m	S/. 40.00
	Cable UTP cat 6	30 m	S/. 60.00
	Conector RJ45 cat 5e	20	S/. 10.00
	Conector RJ45 cat 6	20	S/. 20.00
	Ponchador	1	S/. 20.00
	Software GNS3	1	S/. 0.00
	IOS Cisco	2	S/. 0.00
Servicios	Internet x hora	300	S/. 300.00
Costo Total			**S/. 450.00**

CONCLUSIONES

- El uso del emulador GNS3 a nivel académico es muy útil, debido a que emula equipos ciscos fisicos de tal forma que permite al estudiante interactuar de manera más real y evitando posibles inconvenientes en las configuraciones por no tener comandos no reconocidos o no funcionales.

- El emulador GNS3 puede ser de gran utilidad tanto a nivel empresarial, ya que su uso permite la disminución de equipos, espacio físico y por ende reducción de costos en la implementación de redes.

- GNS3 permite cosas sofisticadas como usar las interfaces del PC como si fueran interfaces del enrutador, de esa manera se puede convertir la interfaz del PC en una interfaz de un enrutador emulado, de tal manera que los protocolos que se ejecutan en el enrutador salen efectivamente por la interfaz del PC.

- Las guías de laboratorio permite al estudiante profundizar los conceptos teóricos vistos en clase, mejorando la capacidad práctica que se requiere en el campo de Networking.

- Al diseñar e implementar la red formada por routers emulados en GNS3 y analizar el rendimiento de la misma enviando paquetes de diferente tamaño, se pudo observar que los valores de los indicadores Latencia y Jitter son superiores a los valores obtenidos en el escenario de routers emulados Físicos.

- Al diseñar e implementar la red formada por routers emulados físicos y analizar el rendimiento de la misma enviando paquetes de diferente tamaño, se pudo observar que los valores de los indicadores Latencia y Jitter propuestos tienen el mejor rendimiento a diferencia del escenario con routers emulados en GNS3.

- Con respecto al trhoughput se sabe que toma menos tiempo transmitir un paquete corto que uno largo, es por eso que todos los dispositivos envían más paquetes cortos durante la prueba. Se comprueba que enlace virtual es más lento y fácilmente congestionable que uno real.

- Un router emulado con GNS3 registra valores de Jitter y latencia muy por encima de los registrados para un router real. Los valores para el router emulado aumentan conforme se envían paquetes de mayor longitud.

GLOSARIO

LAN Una red de área local, red local o LAN (del inglés Local Área Network) es la interconexión de varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros.

WAN Una red WAN, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente o cualquier red en la cual no estén en un mismo edificio todos sus miembros.

ICMP ICMP (Protocolo de mensajes de control de Internet) es un protocolo que permite administrar información relacionada con errores de los equipos en red.

Buffer Un buffer (o búfer) es un espacio de memoria, en el que se almacenan datos para evitar que el programa o recurso que los requiere, ya sea hardware o software, se quede sin datos durante una transferencia.

Telnet Telnet es un protocolo de red que se utiliza para acceder a una computadora y manejarla de forma remota. El término también permite nombrar al programa informático que implementa el cliente.

Emulador Un emulador es un programa destinado a recrear internamente el funcionamiento de una arquitectura diferente a aquella en que se ejecuta. El emulador no es más que un programa sin partes hardware que utilizando los recursos de la máquina donde se ejecuta, simula el comportamiento de un equipo real.

Topología La topología de una red es el arreglo físico o lógico en el cual los dispositivos o nodos de una red (e.g. computadoras, impresoras, servidores, hubs, switches, enrutadores, etc.) se interconectan entre sí sobre un medio de comunicación.

Adaptador de Bucle invertido

El adaptador de bucle invertido de Microsoft es una herramienta para probar en un entorno de red virtual si el acceso a la red es o no factible Además, el adaptador de bucle invertido es esencial si hay conflictos con un adaptador de red o un controlador de adaptador de red.

Trama

Es una serie sucesiva de bits, organizados en forma cíclica, que transportan información y que permiten en la recepción extraer esta información.

VOIP

También llamado **Voz sobre IP**, es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet).

Protocolo

Es un conjunto de reglas y normas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellos para transmitir información por medio de cualquier tipo de variación de una magnitud física.

FastEthernet

Fast Ethernet o Ethernet de alta velocidad es el nombre de una serie de estándares de IEEE de redes Ethernet de 100 Mbps (megabits por segundo).

GigabitEthernet

también conocida como **GigaE**, es una ampliación del estándar Ethernet que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a unos 1000 megabits por segundo de rendimiento contra unos 100 de Fast Ethernet (También llamado 100BASE-TX).

Simulación

La simulación es una técnica que imita el funcionamiento de un sistema del mundo real para entender el comportamiento del sistema o evaluar varias estrategias.

ANEXO A

1.- RED FORMADA POR TRES ROUTERS FÍSICOS CON CABLE UTP CATEGORIA 5

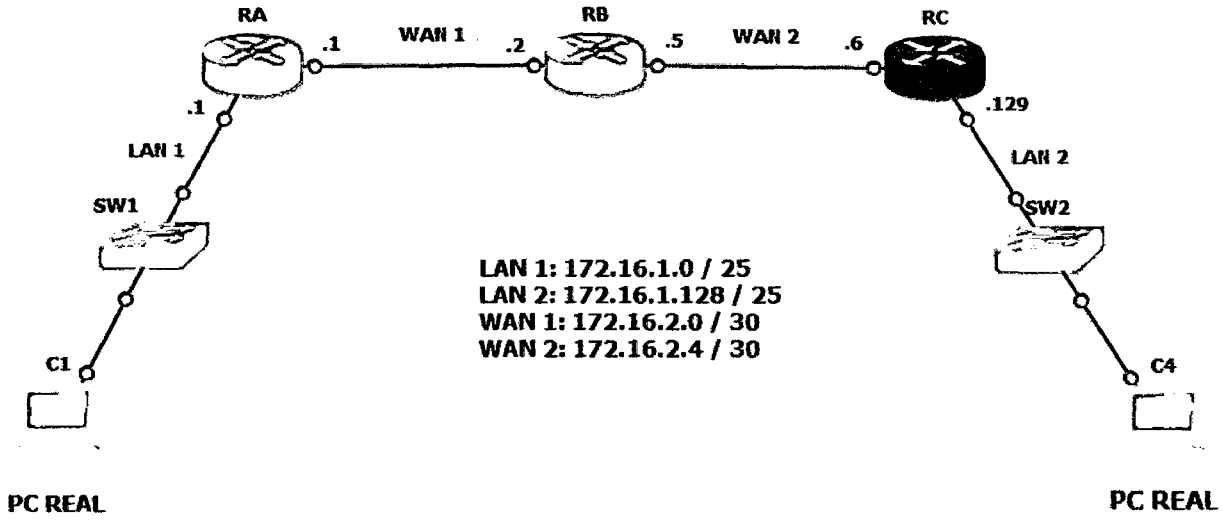


Fig. A.1 Diagrama de topología de red Física.

1.1.- MEDICIÓN DE LA LATENCIA:

LATENCIA											
Tamaño de Trama (bytes)	64										
	N°1	N°2	N°3	N°4	N°5	N°6	N°7	N°8	N°9	N°10	Promedio
Tiempo Mínimo (ms)	1	1	1	1	1	1	1	1	1	1	1
Tiempo Máximo (ms)	1	1	1	1	1	1	1	1	1	1	1
Tiempo Promedio (ms)	1	1	1	1	1	1	1	1	1	1	1

Tabla A.1.1 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	128										
	N°1	N°2	N°3	N°4	N°5	N°6	N°7	N°8	N°9	N°10	Promedio
Tiempo Mínimo (ms)	1	1	1	1	1	1	1	1	1	1	1
Tiempo Máximo (ms)	1	2	2	2	1	1	1	1	1	1	1.3
Tiempo Promedio (ms)	1	1	1	1	1	1	1	1	1	1	1

Tabla A.1.2 Datos obtenidos para una trama de 128 bytes.

LATENCIA											
Tamaño de Trama (bytes)	256										
	Nº1	Nº2	Nº3	Nº4	Nº5	Nº6	Nº7	Nº8	Nº9	Nº10	Promedio
Tiempo Mínimo (ms)	1	1	1	1	1	1	1	1	1	1	1
Tiempo Máximo (ms)	1	2	1	2	1	1	2	1	1	1	1.3
Tiempo Promedio (ms)	1	1	1	1	1	1	1	1	1	1	1

Tabla A.1.3 Datos obtenidos para una trama de 256 bytes.

LATENCIA											
Tamaño de Trama (bytes)	512										
	Nº1	Nº2	Nº3	Nº4	Nº5	Nº6	Nº7	Nº8	Nº9	Nº10	Promedio
Tiempo Mínimo (ms)	1	1	1	1	1	1	1	1	1	1	1
Tiempo Máximo (ms)	1	2	1	2	1	2	2	2	2	1	1.5
Tiempo Promedio (ms)	1	1	1	1	1	1	1	1	1	1	1

Tabla A.1.4 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1024										
	Nº1	Nº2	Nº3	Nº4	Nº5	Nº6	Nº7	Nº8	Nº9	Nº10	Promedio
Tiempo Mínimo (ms)	1	1	1	1	1	1	1	1	1	1	1
Tiempo Máximo (ms)	2	2	2	2	2	2	2	2	2	2	2
Tiempo Promedio (ms)	1	1	1	1	1	1	1	1	1	1	1

Tabla A.1.5 Datos obtenidos para una trama de 1024 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1280										
	Nº1	Nº2	Nº3	Nº4	Nº5	Nº6	Nº7	Nº8	Nº9	Nº10	Promedio
Tiempo Mínimo (ms)	2	2	2	2	2	2	2	2	2	2	2
Tiempo Máximo (ms)	2	2	2	2	2	2	2	2	2	2	2
Tiempo Promedio (ms)	2	2	2	1	2	2	2	2	2	2	2

Tabla A.1.6 Datos obtenidos para una trama de1280 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1518										
	N°1	N°2	N°3	N°4	N°5	N°6	N°7	N°8	N°9	N°10	Promedio
Tiempo Mínimo (ms)	2	2	2	2	2	2	2	2	2	2	2
Tiempo Máximo (ms)	2	2	2	2	3	2	2	3	2	2	2.2
Tiempo Promedio (ms)	2	2	2	2	2	2	2	2	2	2	2

Tabla A.1.7 Datos obtenidos para una trama de 1518 bytes.

LATENCIA							
Tamaño de Trama (bytes)	64	128	256	512	1024	1280	1518
Tiempo Mínimo (ms)	1	1	1	1	1	2	2
Tiempo Máximo (ms)	1	1.3	1.3	1.5	2	2	2.2
Tiempo Promedio (ms)	1	1	1	1	1	2	2

Tabla A.1.8 Comparación de datos obtenidos de las diferentes tramas.

1.2.- MEDICIÓN DEL THROUGHPUT:

THROUGHPUT			
Longitud de Trama (bytes)	750	1125	1500
Velocidad de Tx (Mbps)	1	1	1
Velocidad de Rx (Mbps)	1	1	0.99
Tramas Transmitidas	1666	1112	834
Tramas Recibidas	1666	1112	834
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Tramas Recibidas (pps)	166	111	83

Tabla A.1.9 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	750	1125	1500
Velocidad de Tx (Mbps)	5	5	5
Velocidad de Rx (Mbps)	4.99	5	5
Tramas Transmitidas	8326	5549	4169
Tramas Recibidas	8326	5549	4169
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Tramas Recibidas (pps)	833	555	417

Tabla A.1.10 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	50	50	50
Velocidad de Rx (Mbps)	49.76	49.97	49.90
Tramas Transmitidas	82940	55476	41607
Tramas Recibidas	82688	55442	41589
Tramas Perdidas	252 (0.3%)	34 (0.061%)	18 (0.043%)
Tramas Recibidas (pps)	8294	5548	4160

Tabla A.1.11 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	90	90	90
Velocidad de Rx (Mbps)	82.48	89.14	83.07
Tramas Transmitidas	137561	98967	69337
Tramas Recibidas	137474	98890	69233
Tramas Perdidas	87 (0.063%)	77 (0.078%)	104 (0.15%)
Tramas Recibidas (pps)	113756	9896	6934

Tabla A.1.12 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	1	2	5	10
Velocidad de Rx (Mbps)	1	1.99	5	10
Tramas Transmitidas	851	1700	4247	8494
Tramas Recibidas	851	1700	4247	8494
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)	0 (0%)
Tramas Recibidas (pps)	85	170	425	849

Tabla A.1.13 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

THROUGHPUT				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	20	50	80	90
Velocidad de Rx (Mbps)	19.80	49.47	79.09	89.72
Tramas Transmitidas	16983	42491	67930	76810
Tramas Recibidas	16817	42008	67048	76175
Tramas Perdidas	166 (0.98%)	483 (1.1%)	882 (1.3%)	635 (0.83%)
Tramas Recibidas (pps)	1700	4249	6793	7681

Tabla A.1.14 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

THROUGHPUT				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	91	92	93	94
Velocidad de Rx (Mbps)	90.32	91.07	91.39	80.12
Tramas Transmitidas	77409	77653	78266	70207
Tramas Recibidas	76687	77327	77596	68452
Tramas Perdidas	722 (0.93%)	326 (0.42%)	0 (0.86%)	1755 (2.5%)
Tramas Recibidas (pps)	7740	7765	7827	7020

Tabla A.1.15 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

THROUGHPUT				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	95	100	150	200
Velocidad de Rx (Mbps)	86.01	68.97	75.30	77.86
Tramas Transmitidas	73364	59061	64317	66864
Tramas Recibidas	72910	58376	64035	66106
Tramas Perdidas	454 (0.62%)	685 (1.2%)	282 (0.44%)	758 (1.1%)
Tramas Recibidas (pps)	7336	5906	6432	6686

Tabla A.1.16 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

1.3.- MEDICIÓN DEL JITTER:

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	1	1	1
Velocidad de Rx (Mbps)	1	1	0.99
Tramas Transmitidas	1666	1112	834
Tramas Recibidas	1666	1112	834
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	0.002	0.177	0.726

Tabla A.1.17 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	5	5	5
Velocidad de Rx (Mbps)	4.99	5	5
Tramas Transmitidas	8326	5549	4169
Tramas Recibidas	8326	5549	4169
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	0	0.001	0.001

Tabla A.1.18 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	50	50	50
Velocidad de Rx (Mbps)	49.76	49.97	49.90
Tramas Transmitidas	82940	55476	41607
Tramas Recibidas	82688	55442	41589
Tramas Perdidas	252 (0.3%)	34 (0.061%)	18 (0.043%)
Jitter (ms)	0.918	1.247	1.402

Tabla A.1.19 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	90	90	90
Velocidad de Rx (Mbps)	82.48	89.14	83.07
Tramas Transmitidas	137561	98967	69337
Tramas Recibidas	137474	98890	69233
Tramas Perdidas	87 (0.063%)	77 (0.078%)	104 (00.15%)
Jitter (ms)	0.905	0.917	0.981

Tabla A.1.20 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	1	2	5	10
Velocidad de Rx (Mbps)	1	1.99	5	10
Tramas Transmitidas	851	1700	4247	8494
Tramas Recibidas	851	1700	4247	8481
Tramas Perdidas	0 (0%)	0 (0%)	0 (0 %)	13 (0.15%)
Jitter (ms)	0	0	0	0

Tabla A.1.21 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

JITTER				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	20	50	80	90
Velocidad de Rx (Mbps)	19.80	49.47	79.09	89.72
Tramas Transmitidas	16983	42491	67930	76810
Tramas Recibidas	16817	42008	67048	76175
Tramas Perdidas	166 (0.98%)	483 (1.1%)	882 (1.3%)	635 (0.83%)
Jitter (ms)	0	0.084	0.091	0.973

Tabla A.1.22 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

JITTER				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	91	92	93	94
Velocidad de Rx (Mbps)	90.32	91.07	91.39	80.12
Tramas Transmitidas	77409	77653	78266	70207
Tramas Recibidas	76687	77327	77596	68452
Tramas Perdidas	722 (0.93%)	326 (0.42%)	670 (0.86%)	1755 (2.5 %)
Jitter (ms)	0.92	0.921	0.927	1.115

Tabla A.1.23 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

JITTER				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	95	100	150	200
Velocidad de Rx (Mbps)	86.01	68.97	75305	77.86
Tramas Transmitidas	73364	59061	64317	66864
Tramas Recibidas	72910	58376	64035	66106
Tramas Perdidas	454 (0.62%)	685 (1.2%)	282 (0.44%)	758 (1.1%)
Jitter (ms)	1.057	0.918	1.58	0.918

Tabla A.1.24 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

2.- RED FORMADA POR TRES ROUTERS FÍSICOS CON CABLE UTP CATEGORIA 6

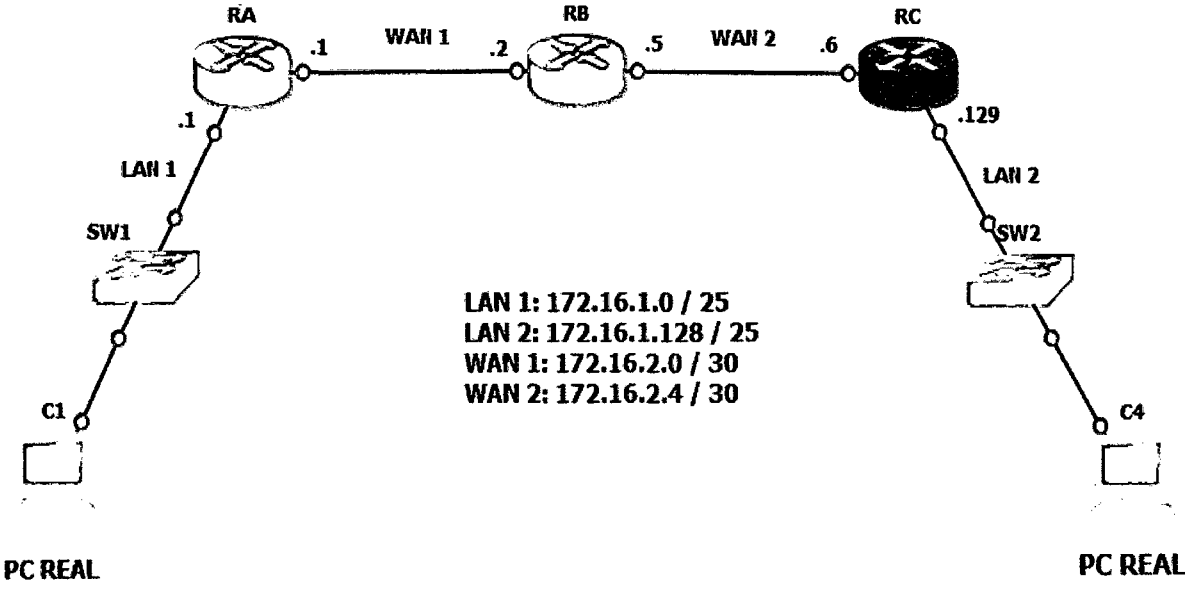


Fig. A.2 Diagrama de topología de red Física.

2.1.- MEDICIÓN DE LA LATENCIA:

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	N° 1	**N° 2**	**N° 3**	**N° 4**	**N° 5**	**N° 6**	**N° 7**	**N° 8**	**N° 9**	**N° 10**	**Promedio**
Tiempo Mínimo (ms)	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1
Tiempo Máximo (ms)	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1
Tiempo Promedio (ms)	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1

Tabla A.2.1 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	128										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1
Tiempo Máximo (ms)	1	<1	1	<1	1	<1	1	1	1	<1	1
Tiempo Promedio (ms)	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1

Tabla A.2.2 Datos obtenidos para una trama de 128 bytes.

LATENCIA											
Tamaño de Trama (bytes)	256										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1
Tiempo Máximo (ms)	1	1	<1	1	1	1	<1	1	1	1	1
Tiempo Promedio (ms)	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1

Tabla A.2.3 Datos obtenidos para una trama de 256 bytes.

LATENCIA											
Tamaño de Trama (bytes)	512										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1
Tiempo Máximo (ms)	1	1	1	1	1	1	1	1	1	1	1
Tiempo Promedio (ms)	<1	<1	<1	1	1	<1	1	1	<1	<1	1

Tabla A.2.4 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1024										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1
Tiempo Máximo (ms)	1	1	1	2	1	2	2	1	1	1	1.3
Tiempo Promedio (ms)	<1	1	<1	1	<1	1	1	<1	<1	1	1

Tabla A.2.5 Datos obtenidos para una trama de 1024 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1280										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1
Tiempo Máximo (ms)	1	2	1	1	2	1	1	2	2	1	1.4
Tiempo Promedio (ms)	<1	1	<1	1	1	<1	1	1	<1	1	1

Tabla A.2.6 Datos obtenidos para una trama de 1280 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1518										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	1	1	1	1	1	1	1	1	1	1	1
Tiempo Máximo (ms)	2	2	2	2	2	2	2	2	2	2	2
Tiempo Promedio (ms)	1	1	1	1	1	1	1	1	1	1	1

Tabla A.2.7 Datos obtenidos para una trama de 1518 bytes.

LATENCIA							
Tamaño de Trama (bytes)	64	128	256	512	1024	1280	1518
Tiempo Mínimo (ms)	<1	<1	<1	<1	<1	<1	1
Tiempo Máximo (ms)	<1	1	1	1	1.3	1.4	2
Tiempo Promedio (ms)	<1	<1	<1	1	1	1	1

Tabla A.2.8 Comparación de datos obtenidos de las diferentes tramas.

2.2.- MEDICIÓN DEL THROUGHPUT

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	5	5	5
Velocidad de Rx (Mbps)	4.99	4.99	5
Tramas Transmitidas	8327	5549	4162
Tramas Recibidas	8327	5549	4162
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Tramas Recibidas (pps)	833	554	416

Tabla A.2.9 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	50	50	50
Velocidad de Rx (Mbps)	49.92	49.74	50
Tramas Transmitidas	83214	55285	41607
Tramas Recibidas	83212	55276	41593
Tramas Perdidas	2 (0.002%)	9 (0.016%)	14 (0.034%)
Tramas Recibidas (pps)	8321	5529	4163

Tabla A.2.10 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	90	90	90
Velocidad de Rx (Mbps)	82.69	89.33	83.17
Tramas Transmitidas	137698	99106	69313
Tramas Recibidas	137698	99103	39313
Tramas Perdidas	0 (0%)	3 (0.003%)	0 (0%)
Tramas Recibidas (pps)	13770	9911	6930

Tabla A.2.11 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	5	10	20	50
Velocidad de Rx (Mbps)	5	10	20	49.82
Tramas Transmitidas	4249	8497	16983	42371
Tramas Recibidas	4249	8497	16983	42371
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)	0 (0%)
Tramas Recibidas (pps)	425	850	1698	4237

Tabla A.2.12 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

THROUGHPUT				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	90	100	100	180
Velocidad de Rx (Mbps)	90	82.54	75.56	90.57
Tramas Transmitidas	76713	67455	64376	77160
Tramas Recibidas	76713	67380	64254	77015
Tramas Perdidas	0 (0%)	75 (0.11%)	122 (0.19%)	145 (0.19%)
Tramas Recibidas (pps)	7671	6745	6436	7716

Tabla A.2.13 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	200	500	1000
Velocidad de Rx (Mbps)	73.64	85.72	89.51
Tramas Transmitidas	66940	72809	76050
Tramas Recibidas	52946	72781	75997
Tramas Perdidas	13994 (21%)	28 (0.038%)	53 (0.7%)
Tramas Recibidas (pps)	6694	7280	7605

Tabla A.2.14 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

2.3.- MEDICIÓN DEL JITTER:

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	5	5	5
Velocidad de Rx (Mbps)	4.99	4.99	5
Tramas Transmitidas	8327	5549	4162
Tramas Recibidas	8327	5549	4162
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	0	0.001	0.001

Tabla A.2.15 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	50	50	50
Velocidad de Rx (Mbps)	49.92	49.74	50
Tramas Transmitidas	83214	55285	41607
Tramas Recibidas	83214	55276	41593
Tramas Perdidas	2 (0.002%)	9 (0.016%)	14 (0.034%)
Jitter (ms)	0	0	0.972

Tabla A.2.16 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	90	90	90
Velocidad de Rx (Mbps)	82.619	89.33	83.17
Tramas Transmitidas	137698	99106	69313
Tramas Recibidas	137698	99103	39313
Tramas Perdidas	0 (0%)	3 (0.003%)	0 (0%)
Jitter (ms)	0.916	0.918	0.966

Tabla A.2.17 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	5	10	20	50
Velocidad de Rx (Mbps)	5	10	20	49.82
Tramas Transmitidas	4249	8497	16983	42371
Tramas Recibidas	4249	8497	16983	42371
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	0.001	0.047	0.574	0.78

Tabla A.2.18 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

JITTER				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	90	100	150	180
Velocidad de Rx (Mbps)	90	82.54	75.65	90.57
Tramas Transmitidas	76713	67455	64376	77160
Tramas Recibidas	76713	67380	64254	77015
Tramas Perdidas	0 (0%)	75 (0.11%)	122 (0.19%)	145 (0.19%)
Jitter (ms)	0.918	0.926	0.957	1.025

Tabla A.2.19 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	200	500	1000
Velocidad de Rx (Mbps)	73.64	85.72	89.51
Tramas Transmitidas	66940	72809	76050
Tramas Recibidas	52946	72781	75997
Tramas Perdidas	13994 (21%)	28 (0.038%)	53 (0.07%)
Jitter (ms)	1.976	0.940	0.917

Tabla A.2.20 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

3.- RED FORMADA POR TRES ROUTERS EN GNS3

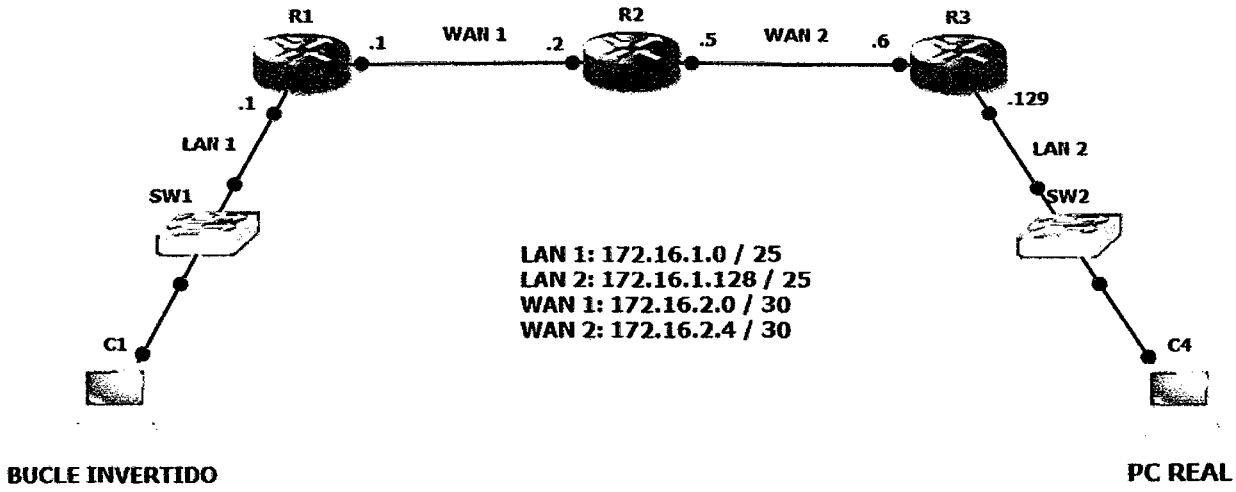


Fig. A.3 Diagrama de topología de red Virtual en GNS3.

3.1.- MEDICIÓN DE LA LATENCIA:

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	37	37	35	36	37	35	36	36	37	36	36.2
Tiempo Máximo (ms)	212	200	339	320	174	235	359	387	225	320	270.1
Tiempo Promedio (ms)	87	91	86	98	84	88	92	84	92	93	89.5

Tabla A.3.1 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**128**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	41	37	39	40	37	38	37	36	35	40	37.9
Tiempo Máximo (ms)	272	237	309	295	327	212	301	249	249	274	272.5
Tiempo Promedio (ms)	94	91	89	92	88	90	91	90	97	97	91.9

Tabla A.3.2 Datos obtenidos para una trama de 128 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**256**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	37	37	41	45	38	36	36	39	36	39	38.4
Tiempo Máximo (ms)	526	251	264	172	203	438	265	114	306	238	277.7
Tiempo Promedio (ms)	98	90	91	89	92	89	93	98	90	95	92.5

Tabla A.3.3 Datos obtenidos para una trama de 256 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**512**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	40	38	39	37	39	40	39	43	38	36	38.9
Tiempo Máximo (ms)	309	220	223	491	191	300	354	196	271	293	284.6
Tiempo Promedio (ms)	95	94	86	101	98	92	91	90	97	90	93.4

Tabla A.3.4 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**1024**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	38	43	41	36	40	45	46	37	36	39	40.1
Tiempo Máximo (ms)	403	511	349	342	410	231	277	293	374	243	343.3
Tiempo Promedio (ms)	95	88	92	100	105	103	119	93	93	94	98.2

Tabla A.3.5 Datos obtenidos para una trama de 1024 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**1280**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	40	36	36	48	37	47	37	44	45	48	41.8
Tiempo Máximo (ms)	510	433	269	422	293	449	423	276	364	247	368.6
Tiempo Promedio (ms)	103	98	86	100	100	90	100	108	119	85	98.9

Tabla A.3.6 Datos obtenidos para una trama de 1280 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1518										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	37	44	49	39	37	40	42	46	39	46	41.9
Tiempo Máximo (ms)	279	545	446	192	280	451	260	459	461	342	371.5
Tiempo Promedio (ms)	97	98	119	95	99	90	95	115	98	97	100.3

Tabla A.3.7 Datos obtenidos para una trama de 1518 bytes.

LATENCIA							
Tamaño de Trama (bytes)	64	128	256	512	1024	1280	1518
Tiempo Mínimo (ms)	36.2	37.9	38.4	38.9	40.1	41.8	41.9
Tiempo Máximo (ms)	270.1	272.5	277.7	284.6	343.3	368.6	371.5
Tiempo Promedio (ms)	89.5	91.9	92.5	93.4	98.2	98.9	100.3

Tabla A.3.8 Comparación de datos obtenidos de las diferentes tramas.

3.2.- MEDICIÓN DEL THROUGHPUT:

THROUGHPUT			
Longitud de Trama (bytes)	750	1125	1500
Velocidad de Tx (Mbps)	1	1	1
Velocidad de Rx (Mbps)	0.99	0.99	1
Tramas Transmitidas	1667	1112	834
Tramas Recibidas	1667	1112	834
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Tramas Recibidas (pps)	167	111	83

Tabla A.3.9 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	750	1125	1500
Velocidad de Tx (Mbps)	2	2	2
Velocidad de Rx (Mbps)	2	2	1.99
Tramas Transmitidas	3330	2222	1666
Tramas Recibidas	3330	2222	1666
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Tramas Recibidas (pps)	333	222	166

Tabla A.3.10 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	1	2	5	9
Velocidad de Rx (Mbps)	0.99	2	4.99	8.98
Tramas Transmitidas	852	1700	4249	7648
Tramas Recibidas	852	1700	4249	7648
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)	0 (0%)
Tramas Recibidas (pps)	85	170	425	765

Tabla A.3.11 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

THROUGHPUT				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	10	11	20	50
Velocidad de Rx (Mbps)	9.51	9.01	8.69	6.15
Tramas Transmitidas	8497	9349	16997	42431
Tramas Recibidas	8497	8807	12748	19194
Tramas Perdidas	0 (0%)	75 (0.8%)	4249 (25%)	23337 (55%)
Tramas Recibidas (pps)	850	935	1700	4243

Tabla A.3.12 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

3.3.- MEDICIÓN DEL JITTER:

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	1	1	1
Velocidad de Rx (Mbps)	0.99	0.99	1
Tramas Transmitidas	1667	1112	834
Tramas Recibidas	1667	1112	834
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	3.359	10.726	14.302

Tabla A.3.13 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	2	2	2
Velocidad de Rx (Mbps)	2	2	1.99
Tramas Transmitidas	3330	2222	1666
Tramas Recibidas	3330	2222	1666
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	2.779	5.230	5.621

Tabla A.3.14 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	1	2	5	9
Velocidad de Rx (Mbps)	0.99	2	4.99	8.98
Tramas Transmitidas	852	1700	4249	7648
Tramas Recibidas	852	1700	4249	7648
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	6.918	3.194	3.522	2.909

Tabla A.3.15 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

JITTER				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	10	11	20	50
Velocidad de Rx (Mbps)	9.51	9.01	8.69	6.15
Tramas Transmitidas	8497	9349	16997	42431
Tramas Recibidas	8497	9274	12748	19084
Tramas Perdidas	0 (0%)	75 (0.8%)	4249 (25%)	23337 (55%)
Jitter (ms)	2.282	2.141	2.370	3.112

Tabla A.3.16 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

4.- RED FORMADA POR UN ROUTER FÍSICO Y DOS ROUTERS GNS3

4.1.- MEDICIÓN DE LA LATENCIA:

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	19	22	23	25	24	22	21	22	21	22	22.1
Tiempo Máximo (ms)	79	96	100	75	89	96	97	94	82	94	90.2
Tiempo Promedio (ms)	50	52	52	51	52	51	51	50	50	50	50.9

Tabla A.4.1 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**128**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	25	23	23	22	26	25	20	25	22	26	23.7
Tiempo Máximo (ms)	97	95	106	99	99	115	75	90	94	88	95.8
Tiempo Promedio (ms)	51	52	50	53	52	50	51	51	52	53	51.5

Tabla A.4.2 Datos obtenidos para una trama de 128 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**256**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	32	29	22	20	26	21	24	22	24	29	24.9
Tiempo Máximo (ms)	100	73	71	84	114	118	96	109	98	104	96.7
Tiempo Promedio (ms)	52	52	53	52	54	50	52	52	52	52	52.1

Tabla A.4.3 Datos obtenidos para una trama de 256 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**512**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	25	26	32	30	23	23	30	27	20	21	25.7
Tiempo Máximo (ms)	66	97	124	108	102	138	109	78	93	88	100.3
Tiempo Promedio (ms)	51	53	55	52	52	54	53	52	54	52	52.8

Tabla A.4.4 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**1024**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	27	23	30	30	27	22	23	31	27	22	26.2
Tiempo Máximo (ms)	97	95	109	77	102	133	84	120	80	128	102.5
Tiempo Promedio (ms)	53	53	55	51	54	55	53	56	51	57	53.8

Tabla A.4.5 Datos obtenidos para una trama de 1024 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**1280**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	26	28	21	21	22	34	23	27	30	33	26.5
Tiempo Máximo (ms)	128	210	107	102	101	90	101	201	108	116	126.4
Tiempo Promedio (ms)	56	59	52	53	55	55	56	55	56	58	55.5

Tabla A.4.6 Datos obtenidos para una trama de 1280 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**1518**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	33	28	32	28	29	34	34	23	23	30	29.4
Tiempo Máximo (ms)	291	174	130	124	128	129	435	103	128	100	174.2
Tiempo Promedio (ms)	59	60	55	55	55	55	61	54	56	55	56.5

Tabla A.4.7 Datos obtenidos para una trama de 1518 bytes.

LATENCIA							
Tamaño de Trama (bytes)	**64**	**128**	**256**	**512**	**1024**	**1280**	**1518**
Tiempo Mínimo (ms)	22.1	23.7	24.9	25.7	26.2	26.5	29.4
Tiempo Máximo (ms)	90.2	95.8	96.7	100.3	102.5	126.4	174.2
Tiempo Promedio (ms)	50.9	51.5	52.1	52.8	53.8	55.5	56.5

Tabla A.4.8 Comparación de datos obtenidos de las diferentes tramas.

ANEXO B

1.- CONFIGURACION DEL PROTOCOLO RIPv2:

1.1 DIAGRAMA DE TOPOLOGIA:

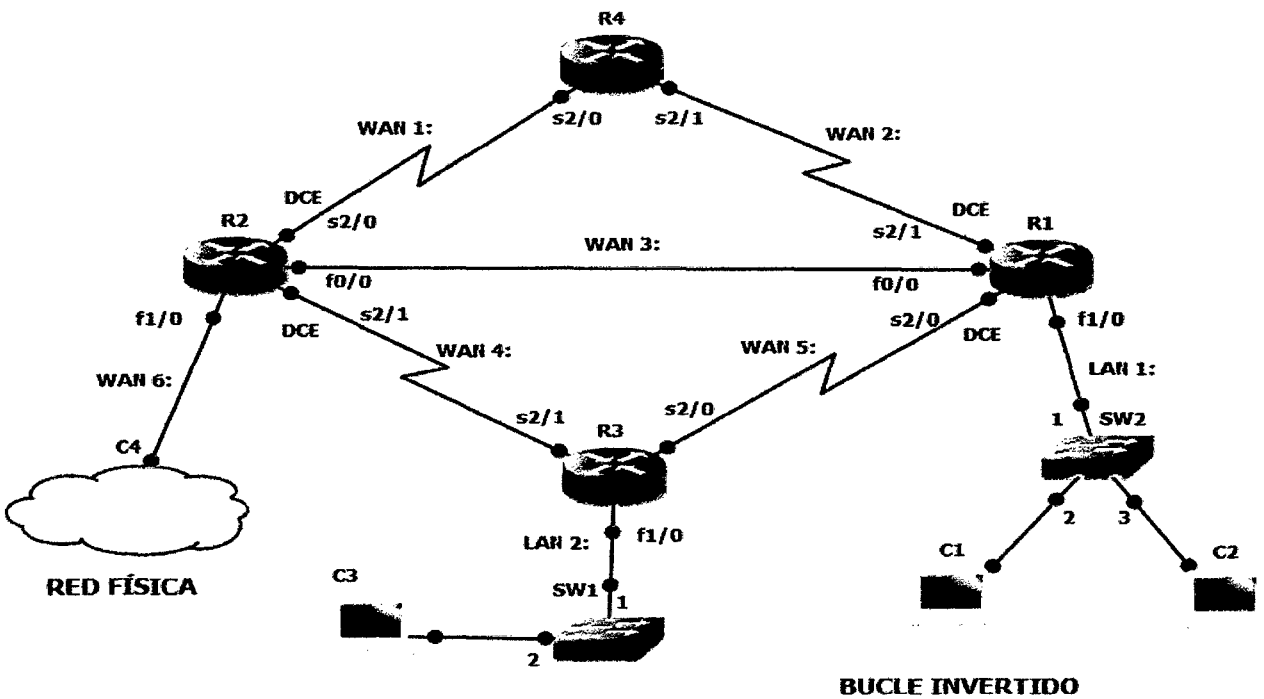


Fig. B.1 Diagrama de topología de red Virtual con RIPv2.

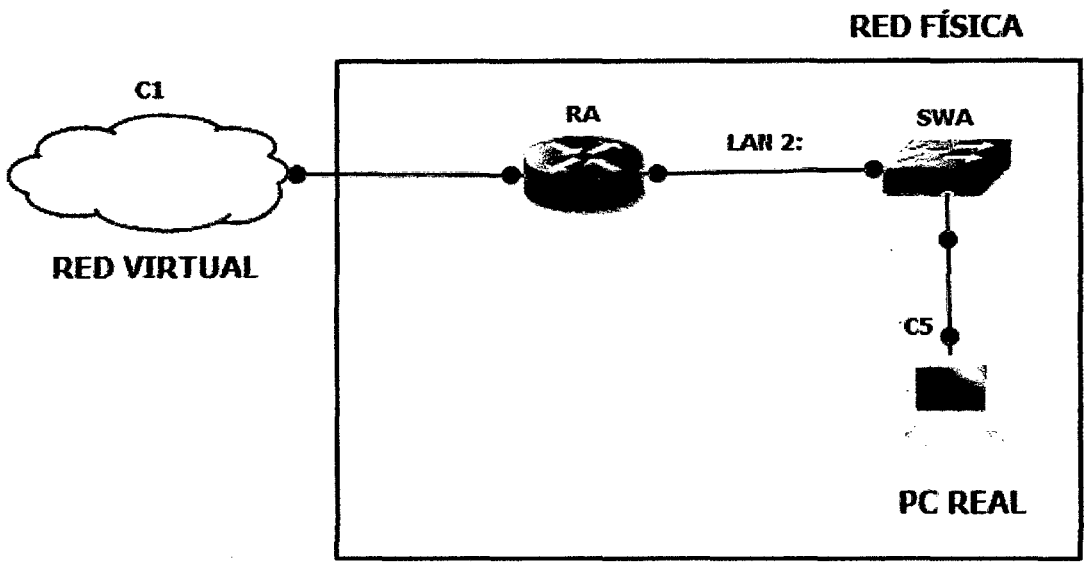


Fig. B.2 Diagrama de topología de red Física con RIPv2.

1.2.- MEDICIÓN DE LA LATENCIA:

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	19	20	18	20	21	22	18	20	17	17	19.2
Tiempo Máximo (ms)	154	223	151	228	179	249	184	312	171	209	216
Tiempo Promedio (ms)	56	60	57	62	47	58	57	60	61	58	57.6

Tabla A.1.1 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**512**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	24	26	22	18	24	20	21	18	23	20	21.6
Tiempo Máximo (ms)	164	405	146	322	314	152	631	284	280	178	287.6
Tiempo Promedio (ms)	55	65	62	59	66	63	54	58	67	59	60.8

Tabla A.1.4 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**1518**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	24	21	26	20	19	24	24	22	20	24	22.4
Tiempo Máximo (ms)	200	251	246	187	507	205	320	223	469	320	292.8
Tiempo Promedio (ms)	58	60	63	58	63	59	62	63	75	80	64.1

Tabla A.1.7 Datos obtenidos para una trama de 1518 bytes.

LATENCIA			
Tamaño de Trama (bytes)	**64**	**512**	**1518**
Tiempo Mínimo (ms)	19.2	21.6	22.4
Tiempo Máximo (ms)	216	287.6	292.8
Tiempo Promedio (ms)	57.6	60.8	64.1

Tabla A.1.8 Comparación de datos obtenidos de las diferentes tramas.

1.3.- MEDICIÓN DEL THROUGHPUT:

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	5	5	5
Velocidad de Rx (Mbps)	5	5	5
Tramas Transmitidas	8334	5557	4168
Tramas Recibidas	8334	5557	4168
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Tramas Recibidas (pps)	835	556	417

Tabla A.1.9 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	1	4	5	10
Velocidad de Rx (Mbps)	1	4	5	10
Tramas Transmitidas	852	3400	4253	8504
Tramas Recibidas	852	3400	4253	8504
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)	0 (0%)
Tramas Recibidas (pps)	85	340	426	850

Tabla A.1.13 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

THROUGHPUT				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	12	15	20	50
Velocidad de Rx (Mbps)	10.83	7.25	5.63	4.029
Tramas Transmitidas	10205	12751	17007	42447
Tramas Recibidas	9455	6330	5064	3512
Tramas Perdidas	750 (7.3%)	6421 (50%)	11943 (70%)	38935(92%)
Tramas Recibidas (pps)	977	1284	1741	4062

Tabla A.1.13 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

1.4.- MEDICIÓN DEL JITTER:

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	5	5	5
Velocidad de Rx (Mbps)	5	5	5
Tramas Transmitidas	8334	5557	4168
Tramas Recibidas	8334	5557	4168
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	2.527	3.089	3.777

Tabla A.1.17 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	1	4	5	10
Velocidad de Rx (Mbps)	1	4	5	10
Tramas Transmitidas	852	3400	4253	8504
Tramas Recibidas	852	3400	4253	8504
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	4.610	3.103	2.812	1.786

Tabla A.1.21 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

JITTER				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	12	15	20	50
Velocidad de Rx (Mbps)	10.83	7.25	5.63	4.029
Tramas Transmitidas	10205	12751	17007	42447
Tramas Recibidas	9455	6330	5064	3512
Tramas Perdidas	750 (7.3%)	6421 (50%)	11943 (70%)	38935(92%)
Jitter (ms)	1.841	2.9	3.083	3.977

Tabla A.1.21 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

2.- CONFIGURACIÓN DEL PROTOCOLO OSPF CON BGP:

2.1 DIAGRAMA DE TOPOLOGIA:

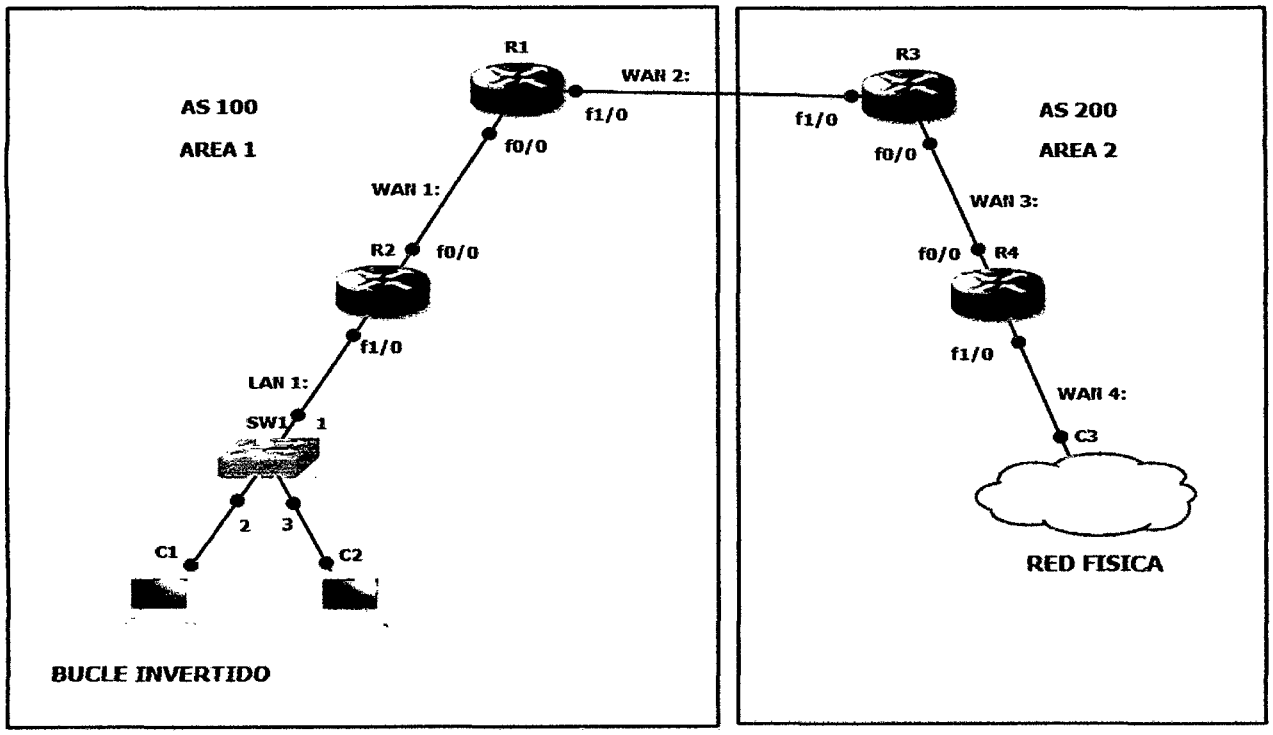


Fig. B.3 Diagrama de topología de red Virtual con OSPF y BGP.

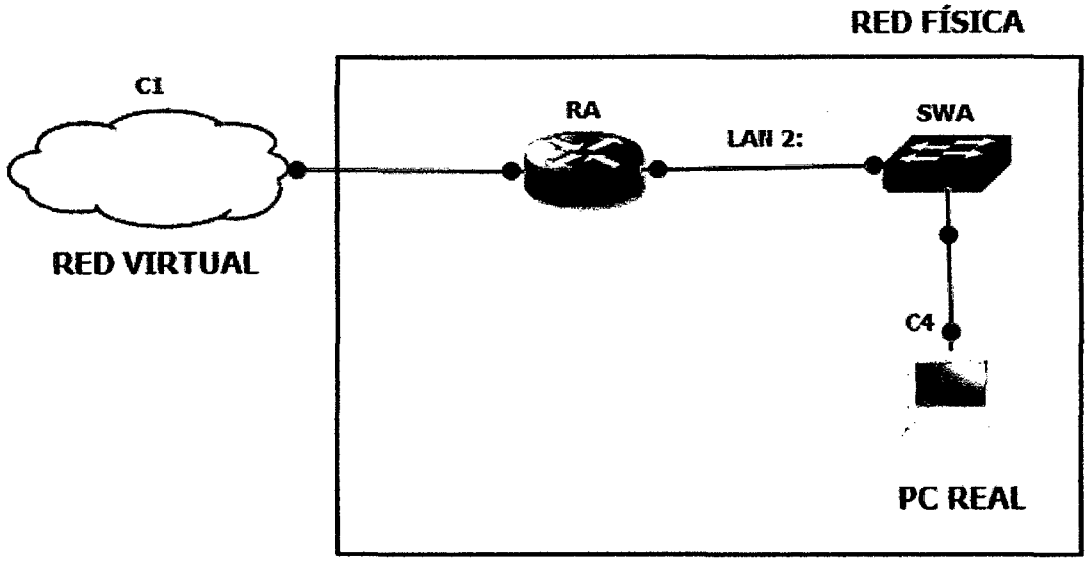


Fig. B.4 Diagrama de topología de red Física con OSPF y BGP.

2.2.- MEDICIÓN DE LA LATENCIA:

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	70	67	66	72	69	71	62	62	71	72	68.2
Tiempo Máximo (ms)	125	227	126	134	203	171	161	250	176	246	181.9
Tiempo Promedio (ms)	94	120	96	102	105	102	102	111	101	116	104.9

Tabla B.2.1 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**512**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	69	70	64	69	68	77	75	73	65	69	69.9
Tiempo Máximo (ms)	353	243	317	215	213	225	205	237	222	227	245.7
Tiempo Promedio (ms)	132	129	138	125	141	128	136	128	130	129	131.6

Tabla B.2.2 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**1518**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	77	71	74	77	69	83	70	81	67	69	73.8
Tiempo Máximo (ms)	394	484	314	564	297	503	226	245	251	440	371.8
Tiempo Promedio (ms)	133	141	126	192	144	170	124	138	137	158	146.3

Tabla B.2.3 Datos obtenidos para una trama de 1518 bytes.

LATENCIA			
Tamaño de Trama (bytes)	**64**	**512**	**1518**
Tiempo Mínimo (ms)	68.2	69.9	73.8
Tiempo Máximo (ms)	181.9	245.7	371.8
Tiempo Promedio (ms)	104.9	131.6	146.3

Tabla B.2.4 Comparación de datos obtenidos de las diferentes tramas.

2.3.- MEDICIÓN DEL THROUGHPUT:

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	3	3	3
Velocidad de Rx (Mbps)	3	3	2.99
Tramas Transmitidas	4994	3330	2498
Tramas Recibidas	4994	3330	2498
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Tramas Recibidas (pps)	500	333	250

Tabla B.2.5 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	1	5	7	10
Velocidad de Rx (Mbps)	1	4.97	6.83	7.24
Tramas Transmitidas	851	4247	5946	8505
Tramas Recibidas	851	4247	5946	8293
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)	212 (2.5%)
Tramas Recibidas (pps)	85	425	594	850

Tabla B.2.6 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

2.4.- MEDICIÓN DEL JITTER:

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	3	3	3
Velocidad de Rx (Mbps)	3	3	2.99
Tramas Transmitidas	4994	3330	2498
Tramas Recibidas	4994	3330	2498
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	0.482	1.011	1.549

Tabla B.2.7 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER				
Longitud de Trama (bytes)	**1470**	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	1	5	7	10
Velocidad de Rx (Mbps)	1	4.97	6.83	7.24
Tramas Transmitidas	851	4247	5946	8505
Tramas Recibidas	851	4247	5946	8293
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	4.226	3.012	2.45	4.331

Tabla B.2.8 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

3.- CONFIGURACIÓN DEL PROTOCOLO OSPF CON PPP:

3.1 DIAGRAMA DE TOPOLOGIA:

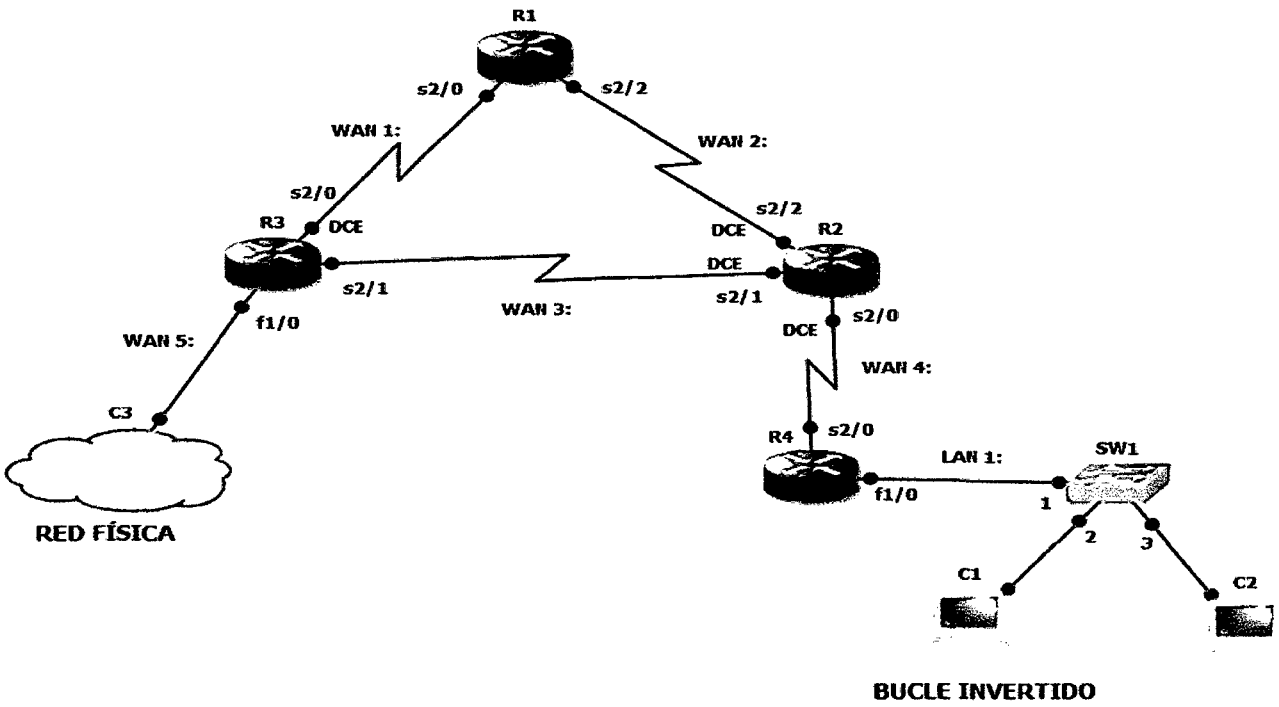


Fig. B.5 Diagrama de topología de red Virtual con OSPF y PPP.

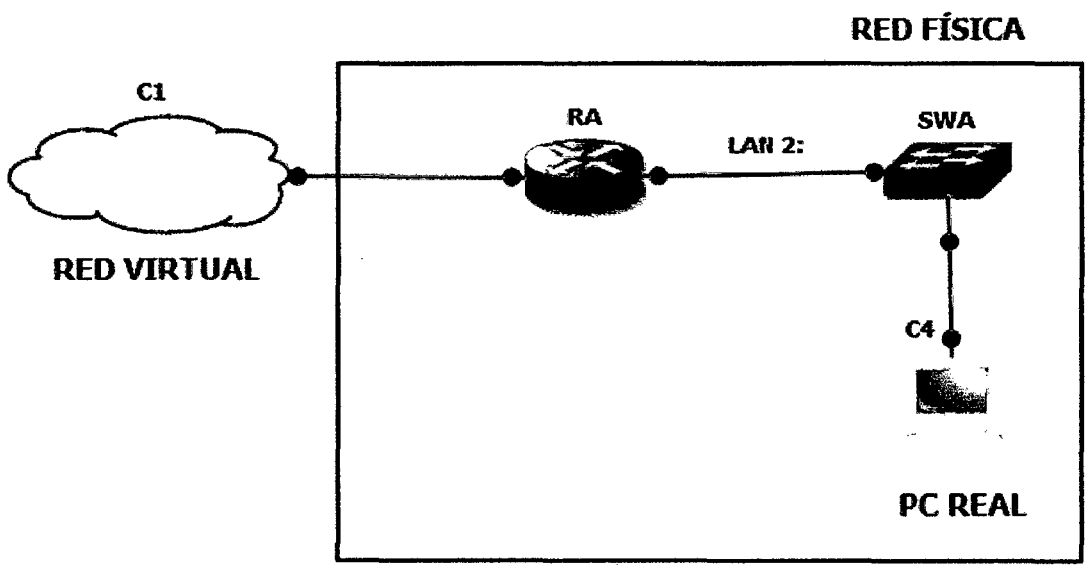


Fig. B.6 Diagrama de topología de red Física con OSPF y PPP.

3.2.- MEDICIÓN DE LA LATENCIA:

LATENCIA											
Tamaño de Trama (bytes)	64										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	66	64	61	59	58	63	61	60	57	62	61.1
Tiempo Máximo (ms)	368	328	461	294	263	268	344	358	235	267	318.6
Tiempo Promedio (ms)	140	121	135	119	140	116	143	126	113	118	127.1

Tabla B.3.1 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	512										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	74	77	71	76	71	64	58	61	63	58	67.3
Tiempo Máximo (ms)	422	544	526	610	593	337	388	359	351	384	451.4
Tiempo Promedio (ms)	228	254	251	241	178	165	166	160	163	168	197.4

Tabla B.3.2 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	1518										
	Nº 1	Nº 2	Nº 3	Nº 4	Nº 5	Nº 6	Nº 7	Nº 8	Nº 9	Nº 10	Promedio
Tiempo Mínimo (ms)	78	90	79	76	83	81	78	71	77	80	79.3
Tiempo Máximo (ms)	674	543	422	637	650	614	569	490	428	537	556.4
Tiempo Promedio (ms)	290	300	156	233	224	241	188	217	150	174	217.3

Tabla B.3.3 Datos obtenidos para una trama de 1518 bytes.

LATENCIA			
Tamaño de Trama (bytes)	64	512	1518
Tiempo Mínimo (ms)	61.1	67.3	79.3
Tiempo Máximo (ms)	318.6	451.4	556.4
Tiempo Promedio (ms)	127.1	197.4	217.3

Tabla B.3.4 Comparación de datos obtenidos de las diferentes tramas.

3.3.- MEDICIÓN DEL THROUGHPUT:

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	0.5	0.5	0.5
Velocidad de Rx (Mbps)	0.5	0.497	0.496
Tramas Transmitidas	834	557	418
Tramas Recibidas	834	557	418
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Tramas Recibidas (pps)	84	56	41

Tabla B.3.5 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	0.5	1	2
Velocidad de Rx (Mbps)	0.5	0.924	1.21
Tramas Transmitidas	426	851	1701
Tramas Recibidas	426	851	1613
Tramas Perdidas	0 (0%)	0 (0%)	88 (5.2%)
Tramas Recibidas (pps)	43	84	170

Tabla B.3.6 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

3.4.- MEDICIÓN DEL JITTER:

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	0.5	0.5	0.5
Velocidad de Rx (Mbps)	0.5	0.497	0.496
Tramas Transmitidas	834	557	418
Tramas Recibidas	834	557	418
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	14.226	20.952	26.823

Tabla B.3.7 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	0.5	1	2
Velocidad de Rx (Mbps)	0.5	0.924	1.21
Tramas Transmitidas	426	851	1701
Tramas Recibidas	426	851	1613
Tramas Perdidas	0 (0%)	0 (0%)	88 (5.2%)
Jitter (ms)	17.965	17.481	21.659

Tabla B.3.8 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

4.- CONFIGURACIÓN DEL PROTOCOLO EIGRP CON FRAME RELAY:

4.1 DIAGRAMA DE TOPOLOGIA:

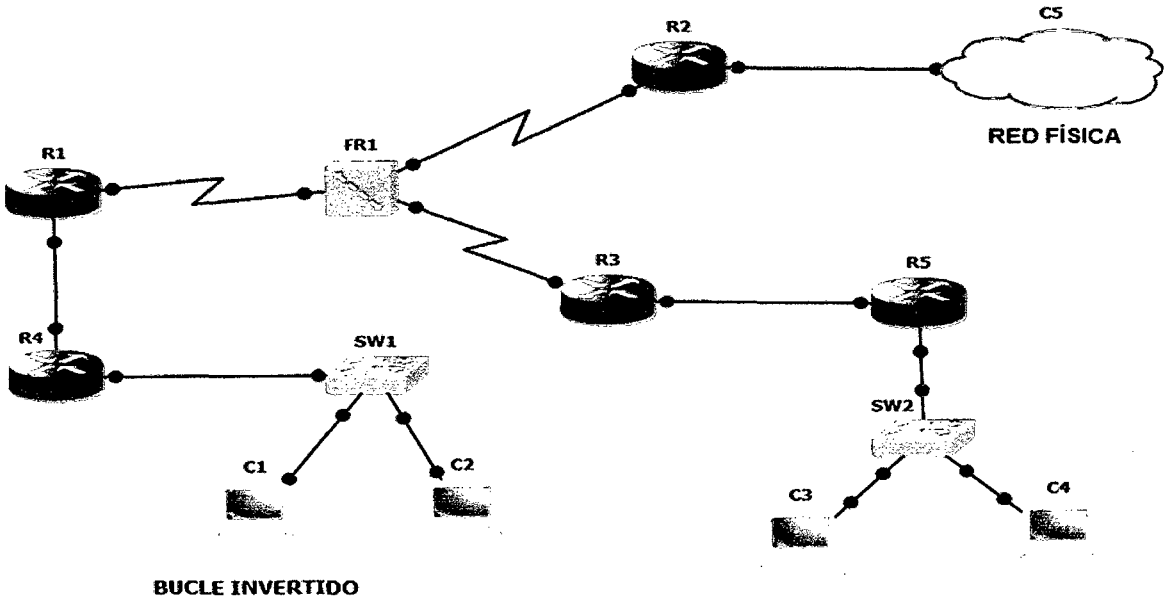


Fig. B.7 Diagrama de topología de red Virtual con EIGRP y FRAME RELAY.

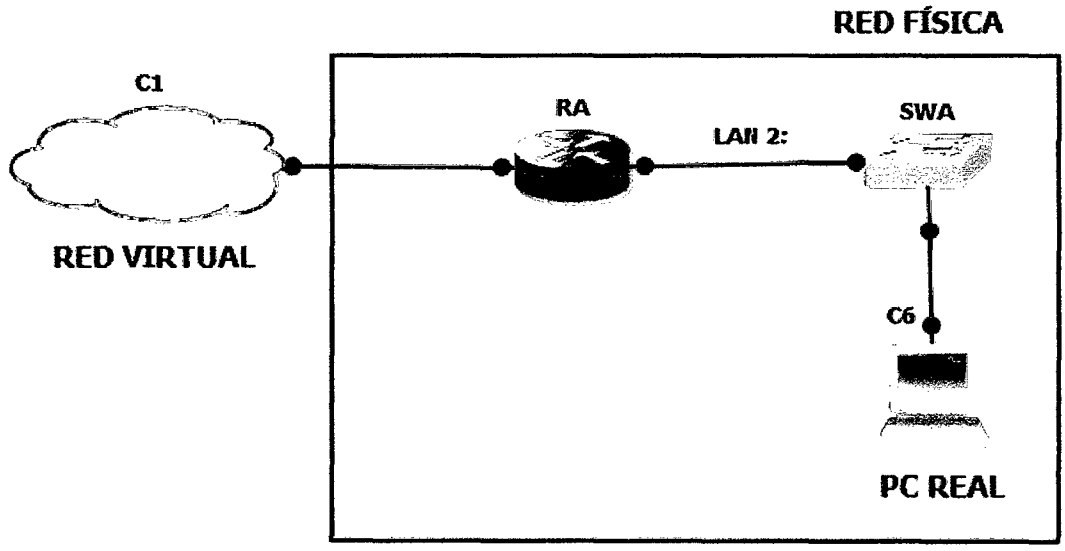


Fig. B.8 Diagrama de topología de red Física con OSPF y FRAME RELAY.

4.2.- MEDICIÓN DE LA LATENCIA:

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	51	51	53	55	50	50	60	53	51	55	52.9
Tiempo Máximo (ms)	288	369	364	422	421	503	346	343	412	284	375.2
Tiempo Promedio (ms)	124	134	118	121	124	120	125	124	118	121	122.9

Tabla B.4.1 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**512**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	53	66	49	51	58	52	48	54	58	51	54
Tiempo Máximo (ms)	496	531	446	421	525	248	279	413	389	270	401.8
Tiempo Promedio (ms)	127	119	120	144	137	128	130	126	172	109	131.2

Tabla B.4.2 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**1518**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	53	57	60	56	56	58	55	57	60	55	56.7
Tiempo Máximo (ms)	300	448	373	334	424	389	602	691	353	250	416.4
Tiempo Promedio (ms)	167	121	144	135	129	145	150	183	120	111	140.5

Tabla B.4.3 Datos obtenidos para una trama de 1518 bytes.

LATENCIA			
Tamaño de Trama (bytes)	**64**	**512**	**1518**
Tiempo Mínimo (ms)	52.9	54	56.7
Tiempo Máximo (ms)	375.2	401.8	416.4
Tiempo Promedio (ms)	122.9	131.2	140.5

Tabla B.4.4 Comparación de datos obtenidos de las diferentes tramas.

4.3.- MEDICIÓN DEL THROUGHPUT:

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	0.5	0.5	0.5
Velocidad de Rx (Mbps)	0.49	0.5	0.5
Tramas Transmitidas	834	556	418
Tramas Recibidas	834	556	418
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Tramas Recibidas (pps)	83	55	41

Tabla B.4.5 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	0.5	1	2
Velocidad de Rx (Mbps)	0.49	1	2
Tramas Transmitidas	426	851	1700
Tramas Recibidas	426	851	1700
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Tramas Recibidas (pps)	43	85	170

Tabla B.4.6 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

4.4.- MEDICIÓN DEL JITTER:

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	0.5	0.5	0.5
Velocidad de Rx (Mbps)	0.49	0.5	0.5
Tramas Transmitidas	834	556	418
Tramas Recibidas	834	556	418
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	5.378	3.809	1.708

Tabla B.4.7 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	0.5	1	2
Velocidad de Rx (Mbps)	0.49	1	2
Tramas Transmitidas	426	851	1700
Tramas Recibidas	426	851	1700
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	8.183	6.65	2.25

Tabla B.4.8 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

5.- CONFIGURACIÓN DEL PROTOCOLO OSPF CON NAT y DHCP:

5.1 DIAGRAMA DE TOPOLOGIA:

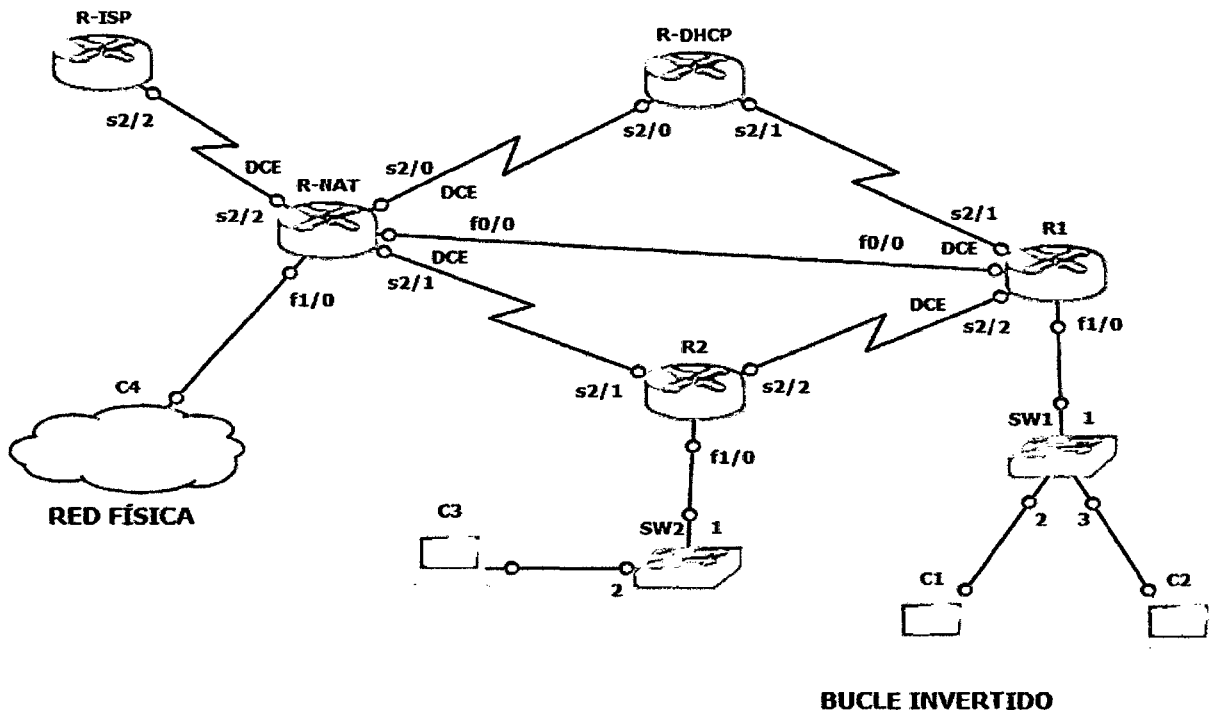


Fig. B.9 Diagrama de topología de red Virtual con OSPF, NAT y DHCP.

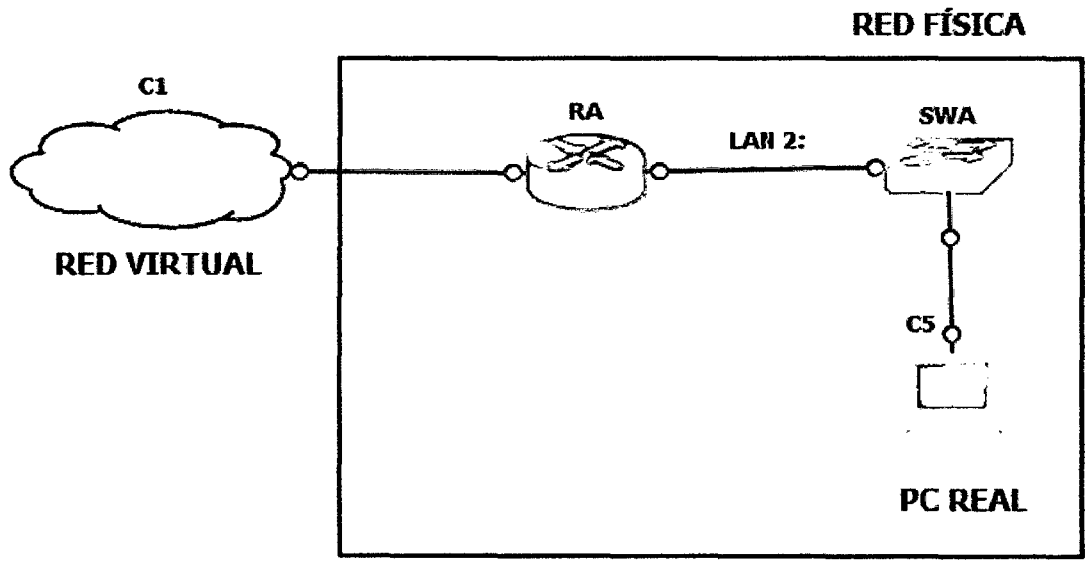


Fig. B.10 Diagrama de topología de red Física con OSPF, NAT y DHCP.

5.2.- MEDICIÓN DE LA LATENCIA:

LATENCIA											
Tamaño de Trama (bytes)	**64**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	47	48	44	48	44	49	48	47	47	47	46.9
Tiempo Máximo (ms)	230	232	432	313	390	145	263	303	331	146	278.5
Tiempo Promedio (ms)	92	96	102	76	80	66	82	71	76	67	80.8

Tabla B.5.1 Datos obtenidos para una trama de 64 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**512**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	45	49	47	49	48	47	46	49	48	48	47.7
Tiempo Máximo (ms)	356	209	199	167	260	504	208	273	329	563	306.8
Tiempo Promedio (ms)	78	72	75	69	72	108	86	89	74	114	83.7

Tabla B.5.2 Datos obtenidos para una trama de 512 bytes.

LATENCIA											
Tamaño de Trama (bytes)	**1518**										
	Nº 1	**Nº 2**	**Nº 3**	**Nº 4**	**Nº 5**	**Nº 6**	**Nº 7**	**Nº 8**	**Nº 9**	**Nº 10**	**Promedio**
Tiempo Mínimo (ms)	42	47	51	54	50	49	51	48	48	52	49.2
Tiempo Máximo (ms)	335	490	545	379	355	338	399	562	634	473	451
Tiempo Promedio (ms)	105	118	102	127	115	141	105	97	136	137	118.3

Tabla B.5.3 Datos obtenidos para una trama de 1518 bytes.

LATENCIA			
Tamaño de Trama (bytes)	**64**	**512**	**1518**
Tiempo Mínimo (ms)	46.9	47.7	49.2
Tiempo Máximo (ms)	278.5	306.8	451
Tiempo Promedio (ms)	80.8	83.7	118.3

Tabla B.5.4 Comparación de datos obtenidos de las diferentes tramas.

5.3.- MEDICIÓN DEL THROUGHPUT:

THROUGHPUT			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	2	2	2
Velocidad de Rx (Mbps)	1.99	2	2
Tramas Transmitidas	3330	2220	1667
Tramas Recibidas	3330	2220	1667
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Tramas Recibidas (pps)	333	222	166

Tabla B.5.5 Datos obtenidos de throughput para diferentes longitudes de trama.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	1	2	6
Velocidad de Rx (Mbps)	0.99	1.99	6
Tramas Transmitidas	851	1700	5096
Tramas Recibidas	851	1700	5096
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Tramas Recibidas (pps)	85	170	510

Tabla B.5.6 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

THROUGHPUT			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	9	10	11
Velocidad de Rx (Mbps)	9	10	10.56
Tramas Transmitidas	7648	8497	9348
Tramas Recibidas	7648	8497	
Tramas Perdidas	0 (0%)	0 (0%)	245 (2.6%)
Tramas Recibidas (pps)	766	850	932

Tabla B.5.7 Datos obtenidos de Throughput para una longitud de trama de 1470 bytes.

5.4.- MEDICIÓN DEL JITTER:

JITTER			
Longitud de Trama (bytes)	**750**	**1125**	**1500**
Velocidad de Tx (Mbps)	2	2	2
Velocidad de Rx (Mbps)	1.99	2	2
Tramas Transmitidas	3330	2220	1667
Tramas Recibidas	3330	2220	1667
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	1.851	0.379	0.002

Tabla B.5.8 Datos obtenidos de Jitter para diferentes longitudes de trama.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	1	2	6
Velocidad de Rx (Mbps)	0.99	1.99	6
Tramas Transmitidas	851	1700	5096
Tramas Recibidas	851	1700	5096
Tramas Perdidas	0 (0%)	0 (0%)	0 (0%)
Jitter (ms)	1.394	0.177	0.049

Tabla B.5.9 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

JITTER			
Longitud de Trama (bytes)	**1470**	**1470**	**1470**
Velocidad de Tx (Mbps)	9	10	11
Velocidad de Rx (Mbps)	9	10	10.56
Tramas Transmitidas	7648	8497	9348
Tramas Recibidas	7648	8497	9105
Tramas Perdidas	0 (0%)	0 (0%)	243 (2.6%)
Jitter (ms)	0	0	2.53

Tabla B.5.10 Datos obtenidos de Jitter para una longitud de trama de 1470 bytes.

BLIBLIOGRAFIA

1. Módulos de CCNA Cisco
2. Tesis de Referencia 1:
   http://upcommons.upc.edu/pfc/bitstream/2099.1/9989/1/PFC_Lisset_D%C3%ADaz.pdf
3. Tesis de Referencia 2:
   http://186.42.96.211:8080/xmlui/bitstream/handle/123456789/1527/Tesis%20Fernanda%20Tamayo%20Dominguez.pdf?sequence=1
4. TUTORIAL GNS3 ESPAÑOL:
   http://iloo.files.wordpress.com/2009/07/gns3-0-4-1_documentation_spanish.pdf
5. Web GNS3:
   http://www.gns3.net/
6. Tutorial JPERF:
   http://openmaniak.com/es/iperf.php
8. Tutorial PRTG:
   http://www.enerit.net/monitoreo-y-helpdesk/prtg-network-monitor
9. Enrutamiento:

http://upcommons.upc.edu/pfc/bitstream/2099.1/11730/1/PFC.pdf

10. Direccionamiento de Red y Mascara de Sub Red:
    http://los9mm.over-blog.es/article-29399073.html
11. VLSM y CIDR:
    http://mikrotikxperts.com/index.php/2013-03-28-19-49-36/conocimientos-basicos/160-tutorial-vlsm-cidr
12. DHCP:
    http://www.see-my-ip.com/tutoriales/protocolos/dhcp.php
13. BGP:
    http://www.guillesql.es/Articulos/Manual_Cisco_CCNA_Protocolos_Enrutamiento.aspx
14. MPLS:

    http://upcommons.upc.edu/pfc/bitstream/2099.1/11730/1/PFC.pdf